NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WIRELESS LOCAL NETWORK ARCHITECTURE FOR NAVAL MEDICAL TREATMENT FACILITIES

by

Russell C. Deason III

September 2004

Thesis Advisor:	Alex Bordetsky
Second Reader:	Glenn Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Wireless Local Network Architecture for Naval Medical Treatment Facilities	**5. FUNDING NUMBERS**
6. AUTHOR(S) Russell C. Deason III	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

In today's Navy Medicine, an approach towards wireless networks is coming into view. The idea of developing and deploying workable Wireless Local Area Networks (WLAN) throughout Naval hospitals is but just a few years down the road. Currently Naval Medical Treatment Facilities (MTF) are using wired Local Area Networks (LANs) throughout the infrastructure of each facility.

Civilian hospitals and other medical treatment facilities have been experimenting with the concept of WLAN for the past few years. The concept is not new within the Department of Defense. The thought of utilizing wireless technology within a Naval MTF has been challenged by many different situations that have hindered its opportunity of arriving on the scene at an earlier time. The use of wireless technology within a Naval MTF is boundless at this time. With newer capabilities being developed every few months or so, the time grows closer when WLANs will be apart of normal day to day operations for medical staff, administrators, and executives within Navy Medicine.

This thesis will take a look at the architecture of an 802.11x WLAN within a Naval MTF from a "macro" view. It will observe the requirements and needs assessment, along with the pros and cons of wireless that drive Navy Medicine towards the development and deployment of wireless 802.11x technologies. It will also review current technology, architecture, and policies that help in the decision making process. Last, this thesis will look at the cost benefits along with a developmental plan to help in determining if wireless is the way to go for a Naval Medicine.

14. SUBJECT TERMS WLAN, 802.11, Wireless, Local Area Networks	**15. NUMBER OF PAGES** 119
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WIRELESS LOCAL NETWORK ARCHITECTURE FOR NAVAL MEDICAL TREATMENT FACILITIES

Russell C. Deason III
Lieutenant, United States Navy
B.S., Embry-Riddle Aeronautical University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Russell C. Deason III

Approved by: Alex Bordetsky
Thesis Advisor

Glenn Cook
Second Reader/Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In today's Navy Medicine, an approach towards wireless networks is coming into view. The idea of developing and deploying workable Wireless Local Area Networks (WLAN) throughout Naval hospitals is but just a few years down the road. Currently Naval Medical Treatment Facilities (MTF) are using wired Local Area Networks (LANs) throughout the infrastructure of each facility.

Civilian hospitals and other medical treatment facilities have been experimenting with the concept of WLAN for the past few years. The concept is not new within the Department of Defense. The thought of utilizing wireless technology within a Naval MTF has been challenged by many different situations that have hindered its opportunity of arriving on the scene at an earlier time.

The use of wireless technology within a Naval MTF is boundless at this time. With newer capabilities being developed every few months or so, the time grows closer when WLANs will be apart of normal day to day operations for medical staff, administrators, and executives within Navy Medicine.

This thesis will take a look at the architecture of an 802.11x WLAN within a Naval MTF from a "macro" view. It will observe the requirements and needs assessment, along with the pros and cons of wireless that drive Navy Medicine towards the development and deployment of wireless 802.11x technologies. It will also review current technology, architecture, and policies that help in the decision making process. Last, this thesis will look at the cost benefits along with a developmental plan to help in determining if wireless is the way to go for Naval Medicine.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

First, I would like to thank God for my life. Second, I would like thank the Navy for giving me this opportunity to go to school. Third, I would like to thank my professors for their guidance throughout my time here at NPS. Last, but just as important, I would like to thank my family. Without them I know I would not be here striving to make a better life for them and myself. My wife Tabitha and my daughters, Courtney and Brianna, truly are my inspirations to keep going, and for that I will always be grateful.

THIS PAGE INTENTIONALLY LEFT BLANK

I. BACKGROUND/RELATED WORK

A. INTRODUCTION

1. Purpose

The purpose of this thesis is to identify whether or not 802.11x Wireless Local Area Networks are a feasible alternative for Navy Medicine. This is done by taking a look at the concept from a macro view to determine what the needs, requirements, and environments are to develop and deploy such a network throughout Naval Medicine.

2. Research Questions

The questions involved within this paper ask the basics of developing and deploying WLAN architecture. It asks what are the needs and requirements for the deployment of an 802.11x WLAN within an MTF and what are the risks involved? It also asks, “What is the architectural design for the development and deployment of an 802.11x WLAN?” Another question asked is what are the benefits associated with WLANs? The last question asked is what policies are involved in deploying an 802.11x WLAN within a Naval MTF?

3. Scope of Thesis

The scope of this thesis looks at what an 802.11x WLAN can do for Navy Medicine. It answers the question of whether or not it is cost effective, secure, interoperable, accessible, upgradeable, and capable of handling the day to day needs of a Naval MTF. This is a broad brush stroke interpretation of an architectural design. The scope takes a macro view of the overall design of Navy MTFs and looks at the policies, the needs and requirements, and the cost benefit of deploying these types of networks throughout. This thesis does not get into the smaller details of what specific brand of equipment to use. Each MTF is designed differently in regards to size and mission capability, thus equipment will be determined based on each facility. It would not be feasible to draw out every design for each MTF, so the idea of developing a basic template to follow gives Chief Information Officers (CIOs) and other personnel guidelines for developing and deploying a WLAN in accordance with DoD policies.

B. BACKGROUND AND RELATED WORK

1. DoD WLAN Practices

Currently DoD is experimenting with the idea of using 802.11 x wireless within different areas of its operations. Due to classified material, this thesis will not go into specific detail about some of the commands performing these operations. Wireless networks utilizing 802.11x technologies are being deployed on some ships and at specific bases throughout. These ships and bases are performing the beta tests for the rest of the fleet. This will help in determining the vulnerabilities that may arise due to using radio frequencies to distribute data throughout large platforms.

The limitation to all this is policy. The DoD introduced a directive that discusses the use of wireless 802.11x technologies within the DoD Global Information Grid. DoD 8100.2, dated 14 APRIL 04, establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG).[1] It provides the guidelines for deploying and securing data that may be transmitted over the 802.11x frequency. This data does not include any classified material due to the vulnerabilities that are inherited with 802.11x.

COMNAVNETWARCOM NORFOLK VA issued a moratorium on any wireless activity on Navy shore commands. This message came out in July 2004. Along with this message came another message that contained additional guidance for the moratorium. The second message states that "A. WIRELESS TECHNOLOGIES THAT FALL WITHIN THE SCOPE OF THIS MORATORIUM ARE AS FOLLOWS: A) THOSE THAT CAN PERMIT ACCESS TO NAVY INFORMATION SYSTEMS WITHOUT TRANSITING AN EXISTING WIRED NETWORK ACCESS INTERFACE FOR REMOTE CONNECTIVITY, B) THOSE THAT CAN PROVIDE ACCESS TO UNCLASSIFIED DATA STORED ON PORTABLE OR STATIONARY ELECTRONIC DEVICES, AND C) THOSE THAT DO NOT PROTECT THE PRIVACY AND INTEGRITY OF DATA IN TRANSIT (I.E. TRANSMITTING

[1] Directive, Department of Defense, 8100.2. Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG). Pg. 1. April 14, 2004.

OFFICIAL EMAIL INFORMATION IN THE CLEAR WITHOUT APPROVED CRYPTOGRAPHY). PER PARA 4.1.2 OF REF D, EXCEPTIONS MAY BE GRANTED ON A CASE-BY-CASE BASIS AS DETERMINED BY THE NAVY DAA."[2] This means that a wireless network can be implemented, but solid justification has to be in place in order for the Designated Approving Authorities (DAA) to honor such implementation. The additional guidance message helps clarify what is covered in the original message regarding the moratorium. Anyone with existing wireless devices/networks that are covered under current SSAA/IATO/ATO need to be registered by 30 Aug 2004. Appendices C and D are the messages that were sent out.

2. Bureau of Medicine (BUMED) WLAN Practices

At the time of this paper the Bureau of Medicine (BUMED) does not have a policy designed for the deployment of wireless 802.11x technologies. The concept is still new, and since there has been a prohibition to the use of this technology throughout the DoD GIG there has been no need to pursue it. Now that the DoD Directive 8100.2 has been signed, BUMED will have a guideline that will help in the development/deployment of 802.11x WLAN architecture throughout the Naval Medical Training Facilities (MTF).

3. Current MTF Network Architecture

Currently, there is not an MTF WLAN architecture designed as a template for all of Navy Medicine to follow. Permission is given to each practicing or experimenting entity via the Designated Approving Authority (DAA) of each command or region. Only then should a command or person attempt to use wireless in a "business" capacity.

4. Private Health Care WLAN Practices and Policies

The common theme that has presented itself throughout all the articles reviewed for this paper is the need for portability, accessibility, redundancy, and security. There are different variations to the types of wireless systems that are deployed throughout various hospitals within the private sector.

[2] Naval Network Warfare Command. Subj: Additional Guidance for Wireless Local Area Network (WLAN) Moratorium. MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA/-/JUL//. Last accessed July 2004.

Many hospitals that are using wireless are experimenting with the concept of the wireless access control gateway that allows authorized personnel to connect to the Intranet via a Virtual Private Network (VPN).

There is not one company who provides for every need. Each product comes with its own pros and cons. Different vendors provide various pieces of the “pie” to help in operating and securing WLANs.

a. Health Insurance Portability and Accountability Act (HIPAA) of 1996

Every medical facility, including all DoD MTFs, has to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Its design is to ensure the privacy and security of protected health information (PHI) over electronic mediums. Now, wireless itself is not directly mentioned, but “open networks” is. This allows for wireless to fall into the HIPAA guidelines. Specifically, it states that data must be encrypted while on an open network, and ideally would include some mechanism to check the integrity of the transmitted data.[3] The HIPAA statute requires health plans, health care providers, and other covered entities to maintain reasonable and appropriate safeguards to protect individually identifiable health information. Under the HIPAA privacy rules, a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of electronic and non-electronic protected health information. The HIPAA security rules were issued in final form on February 20, 2003. They apply to protected health information in electronic form only. The core principles of the final rules require covered entities to: (1) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any

[3] AirMagnet. Wi-Fi, Health Care, and HIPAA: WLAN Management in the Modern Hospital. Pg.1. Last accessed July 2004.

reasonably anticipated uses or disclosures of such information that are not permitted or required under [the security rules]; and (4) ensure compliance with the [security rules] by its workforce.[4]

Institutions that fall under these guidelines have until April 21, 2005 to be compliant. The exception to this rule is small health institutions. They are granted one more year to allow for compliance.

There are three major areas that HIPAA focuses on. They are (1) Administrative Safeguards, (2) Physical Safeguards, and (3) Technical Safeguards. The first one, Administrative Safeguards (found in Section 164.308) offers regulations for management of healthcare organizations. The next, Physical Safeguards (found in Section 164.310), discusses how secure the facility should be. The third is the area that pertains most to WLANs within an MTF. Technical Safeguards (found in Section 164.312) establishes regulations for access control to networks, integrity and security of data and transmissions, auditing, and last authentication.

In order to provide the highest security to a wireless network, the relevant regulations need to be extracted from the HIPAA document and interpreted for use. The following is a brief summary of the standards that relate.

1. Access control (164.312 (a) (1)) is simply what the name implies, controlling who is granted access to the organization's resources.

2. Auditing (164.312 (b)) is maintaining logs of who accessed a given resource at what time and where so that in the event of a security compromise there will be an audit trail.

3. Integrity (164.312 (c) (1)) consists of making sure that PHI is not modified in any way by an un authorized user during transmission or storage.

[4] Gainer, Randy, van Eckhardt, Michael, Will, Rebecca, Marks, Richard. HIPAA and WiFi – Regulatory Tangles for Wireless Health Care Networks. [http://articles.corporate.findlaw.com/articles/file/00010/008895]. Last accessed July 2004.

4. Person authentication (164.312 (d)) is authenticating that the person the computer says they are really the correct person. This could be argued that it should be done at the server, but I think we can take it a step further and authorize the user when they transition from the wireless to the wired network.

5. Transmission security (164.312 (e) (1)) is ensuring that the network transmissions are kept private and since the media is the air this is a high priority in wireless environments.[5]

HIPPA has demonstrated what it requires from each medical facility to have prior to its deadline. Table 1 gives a brief summary of what is required by each medical facility. Table 1 also provides some solutions for the requirements. These types of requirements will be discussed further within the security portion of this paper.

HIPPA Requirements	Available Solutions
Privacy and Integrity throughout all patient data.	• Wired Equivalent Privacy (WEP) • Wi-Fi Protected Access (WPA) • Virtual Private Networks (VPN)
Detection of intrusions and other unwarranted network activity must be found and alerted.	An Intrusion Detection System that monitors, alerts, and tracks unauthorized activity along the network.
Periodical checks of IDS must be performed to find new vulnerabilities.	System tests along with results and findings should be performed on a regular basis.
Policies and findings from tests must be documented to measure effectiveness of security system.	A security plan that documents how PHI will be kept confidential, along with threats, countermeasures, and training will be created.

Table 1. HIPPA Requirements with Solution.

[5] O'Dorisio, Daniel. Securing Wireless Networks for HIPAA Compliance. Version 1.4 Option 2 (Case Study). SANS Institute. Pg. 3. December 23, 2003.

C. SUMMARY

It is up to BUMED and its affiliates to create a policy for Navy Medicine to follow in order for WLANs to operate at MTFs. Directives have been laid out for the use of commercial WLAN products within DoD. Compliance with these directives along with HIPAA makes it possible to implement a WLAN within an MTF, but it may become difficult until the first MTFs have been installed with them and the bugs have been worked out. It can be done, because hospitals in the private sector are currently operating them with some success.

THIS PAGE INTENTIONALLY LEFT BLANK

II. REQUIREMENTS ANALYSIS AND NEEDS ASSESSMENT

A. THE DRIVING FORCE OF CHANGE

The driving force behind WLAN comes from the health care provider's need for mobility while performing patient care on a day-to-day basis. The mobility of the health care providers within the MTF provides an important part of the delivery system of patient care. By allowing each to move from treatment room to treatment room without having to sit down at a static desktop display and input lab, x-ray, or other forms gives them greater flexibility with patients. This also helps to increase the amount of patients to be seen, and with wireless mobility health care providers can be right beside the patient to review records or other facets of their job that may concern the patient.

The need for greater bandwidth helps in providing a service to the health care provider by offering more applications that pertain to their area of work. Radiologist can use the bandwidth to review x-rays and other imaging that used to be done stationary at a desk. Now they will have the ability to move throughout the MTF and maintain consistent communication with their personnel and patients, while reviewing x-rays and other radiological applications.

B. BUREAU OF MEDICINE (BUMED)

BUMED is researching the concept of developing and deploying WLANs throughout its MTFs, but further research has to be done. There are many different factors that have to be taken into account prior to deploying. This appears to be decided at the executive level. This is an acquisition concern as well. BUMED's driving force is pretty much the same as any other private sector MTF. Like the hospitals within the private sector, Naval MTFs require much of the same levels of necessity. The need for compliance with DoD Directives and other policies adds to the requirements and needs.

The only difference between the two is the operational aspect of the military. It would be thought that by being a DoD affiliate that there is a little leeway with the policies, but since the subject is about protected health information (PHI) there is very little leeway due to the other regulations that cover military medicine in general.

C. MTF STAFF

From a health care provider's perspective the need for wireless would allow them more mobility throughout their clinic or ward. There are many applications that could be used with wireless that allows the doctor to perform the same functions on a wireless PDA or Tablet PC that are already performed from a desktop. Some of these functions involve order labs, x-rays, retrieving past medical history. This concept of moving from floor to floor would work well for all medical personnel who utilize network data for their day to day use. Being stuck behind a desk to review or order patient related data can be time consuming. This paperwork often overwhelms healthcare staff, taking 50-70 percent of their time.[6]

D. SUMMARY

Mobility, along with optimization of time and accuracy, create the driving forces that many MTFs need within a cost restrictive environment that is currently in place. The ability to stay mobile provides a great advantage for the health care provider who is dedicated to patient care. Therefore, the MTF receives more"bang for the buck" with their health care providers.

[6] Geier, Jim. Applications of Wireless Networks. [http://www.wireless-nets.com/papers/wireless_network_applications.htm]. Last accessed July 2004.

III. OPERATIONAL FAMILIARIZATION

A. THE IEEE 802.11 WIRELESS FREQUENCY

1. Introduction

802.11 is an off-spring of some of the earliest wireless technology that dates back to the early 1900s. Actually, it is also a work group that is dedicated to the development of 802.11 frequencies with the goal of providing secure mobile communication. Within 802.11 there are several different groups working to develop different variations of the 802.11 model. They range from 802.11 itself, to a, b, and g. There are others, but these will be the ones we will focus on.

802.11 was the first to be developed. It specifically covers the operation of the media access control (MAC) and physical layers. 802.11 also cover three physical layers. The one that is focused on in this paper is the Direct Sequence Spread Spectrum (DSSS). DSSS functions by dividing the data onto several pieces and simultaneously sending the pieces on as many different frequencies as possible, unlike FHSS, which sends on a limited number of frequencies. This process allows for greater transmission rates than FHSS, but is vulnerable to greater occurrences of interference. This is because the data is spanning a larger portion of the spectrum at any given time than FHSS. In essence, DSSS floods the spectrum all at one time, whereas FHSS selectively transmits over certain frequencies.[7]

The 802.11 standard provides MAC and PHY (Physical Layer) functionality for wireless connectivity of fixed, portable, and moving stations moving at pedestrian and vehicular speeds within a local area. Specific features of the 802.11 standard include the following:

- Support of asynchronous and time-bounded delivery service.
- Continuity of service within extended areas via a distribution system, such as Ethernet.

[7] Wheat, J. and others. Designing a Wireless Network. Pg. 125-126. Syngress, 2002.

- Accommodation of transmission rates of 1Mbps and 2Mbps (802.11a and 802.11b extensions offer higher data rates than the base standard).
- Support of most market applications.
- Multicast (including broadcast services.
- Network management services.
- Registration and authentication services.[8]

802.11a provides a throughput of 54 Mbps (24 Mbps average) with a range of approximately 50 – 100 feet. It was created due to the overwhelming demand for more bandwidth and the growing number of technologies operating within the 2.4 GHz band. 802.11a was created for WLAN use in North America as an alternative to 802.11b, which operates at the 2.4 GHz band. It is not backward compatible with 802.11. 802.11a operates at the 5 GHz band. This reduces the chance of interference. 802.11a is expensive. It is estimated that future versions will exceed 100Mbps.

802.11b is the most common amongst Commercial-Off-The-Shelf (COTS) wireless products. It operates on the 2.4 GHz band, which is considered the Industrial, Scientific, and Medical band. This band is unlicensed; therefore the chance for interference is increased. Its throughput is 11Mbps (5 Mbps average). The average is based on its half-duplex configuration. Its range is around 200-300 feet.

802.11b uses WEP for security. It is protection, but there have been many successful attempts at cracking WEP. It is not a very good means of deterring script kiddies, or the more harden hacker from gaining access into your wireless network. A WEP key can be deciphered in a matter of hours depending on the hardware and software used for the attack.

802.11g is an easy choice for corporate sites and home users to adopt because it doesn't require an upgrade to client equipment. 802.11g is backward-compatible with 802.11b, and it offers speeds similar to those of 802.11a.[9] It operates on the 2.4 GHz

[8] Geier, Jim. Wireless LANs: Implementing High Performance IEEE 802.11 Networks. Second Edition. Pg.77-78. SAMS Publishing. 2002

[9] IBM. The 802.11g Standard –IEEE. [http://www-106.ibm.com/developerworks/wireless/library/wi-ieee.html]. March 2003.

band, and carries a throughput of 54 Mbps. Its range is 1000 feet under ideal conditions, but on average it is more like 150 – 300 feet.

802.11g uses the same security measure, WEP, to help secure the network. It also uses OFDM, AES, and possibly WPA/Wi-Fi to protect access. OFDM is orthogonal frequency division multiplexing. It is an FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. AES is short for Advanced Encryption Standard, a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced *Rhine Dahl* or *Rain Doll*), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM.[10] Last, WPA/Wi-Fi is defined as a security technology for wireless networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP.[11]

2. Strengths

There are many advantages to using a WLAN with 802.11x technologies. One of these is commonality. 802.11x technologies are more Commercial-Off-The-Shelf products. Other types of wireless technology may be either proprietary, non-interoperable, or comes with an expensive price tag. It may be a combination of them all or just a couple.

Another strength or advantage is the ability to place a wireless access point where a wired connection is unable to be. Many of the MTFs within the Navy are growing in

[10] Wi-Fi Planet. AES. [http://wi-fiplanet.webopedia.com/TERM/A/AES.html]. October 2003.

[11] Mitchell, Bradley. “WPA – Wi-Fi Protected Access”. [http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm]. Last accessed July 2004.

age. This limits the ability to add different "LAN drops" throughout the buildings, thus creating a larger budget for materials and labor cost.

Cost is a driving force that causes any decision making entity to determine what type of network will be implemented. By using wireless, the cost of a network can be reduced considerably. Companies reorganize, resulting in the movement of people, new floor plans, office partitions, and other renovations. These changes often require recabling the network, incurring both labor and material costs. In some cases, the recabling costs of organizational changes are substantial, especially with large enterprise networks. A reorganization rate of 15% each year can result in yearly reconfiguration expenses as high as $250,000 for networks that have 6,000 interconnected devices. The advantage of wireless networking is again based on the lack of cable: You can move the network connection by simply relocating an employee's PC.[12]

3. Weaknesses

Security is always the biggest concern for wireless. The introduction of Wireless Equivalent Privacy was created to help deter anyone from gaining access into a WLAN. The downfall to this is that it is accessible to a Brute Force attack. Access to the network can be performed by utilizing different types of software that are able to infiltrate the wireless network either by poisoning the Address Resolution Protocol, which creates a Man-in-the-middle scenario, or as mentioned in the previous sentence, Brute Force. These attacks will be discussed further in the paper.

Another weakness is interoperability. As vendors look to maintain an edge on competition, there is a need to ensure that their product can operate with other products. When different types of hardware are created to provide service to a specific frequency band there is the possibility of it having non-backwards compatibility. Interoperability of products using the same frequency band not only hurts the company creating the product, but it also hurts the consumer and eventually causes the product to become unused.

[12] Geier, Jim. Wireless LANs: Implementing High Performance IEEE 802.11 Networks. Second Edition. Pg.13. SAMS Publishing. 2002

4. Application to Naval Medical Treatment Facilities

The concept of developing and deploying an 802.11x WLAN within a Naval MTF is possible. The concerns about wireless within an MTF involve compliance with the policies that govern. Not only do policies play a role, but so does interference with other devices using the same signal. 802.11, 802.11b and 802.11g operate on the 2.4 GHz band. This band is called the ISM band (Industrial, Scientific, and Medical). These frequencies reside between 902 MHz and 5.85 GHz, just above the cellular phone operating frequencies. The ISM band is very attractive to wireless network vendors because it provides a part of the spectrum upon which to base their products, and end users do not have to obtain FCC licenses to operate the products.[13]

Throughout many of the wards in an MTF there are devices that broadcast bio-information that is crucial to the survival of patients. The possibility of interfering with either the WLAN or the other devices becomes a concern. To counter this, the idea of shielding the medical equipment from WLAN interference has become the solution. This will be discussed further later in the paper.

B. HARDWARE DEVICES

1. Introduction

The hardware devices discussed within this paper are the devices that are most commonly used throughout all WLANs. These devices are what make a WLAN possible. The hardware devices used for a WLAN piggy back off of an already wired LAN. By piggy backing off of a wired LAN redundancy can occur to ensure that communication and patient care can be performed.

2. Switches

A switch is a small device that joins multiple computers together at a low-level network protocol layer. Technically, network switches operate at layer two (Data Link Layer) of the OSI model. Network switches look nearly identical to hubs, but a switch generally contains more "intelligence" (and a slightly higher price tag) than a hub. Unlike hubs, network switches are capable of inspecting the data packets as they are

[13] Geier, Jim. Wireless LANs: Implementing High Performance IEEE 802.11 Networks. Second Edition. Pg.31. SAMS Publishing. 2002

received, determining the source and destination device of that packet, and forwarding that packet appropriately. By delivering messages only to the connected device that it was intended for, network switches conserve network bandwidth and offer generally better performance than hubs.

As with hubs, Ethernet network switches are the most common. A network switch offers differing port configurations starting with the four- and five-port models, and support 10 Mbps Ethernet, 100 Mbps Ethernet, or both.[14] This is where the WLAN AP will connect prior to broadcasting to wireless MACs. Figure 3.1 is an image of a switch.

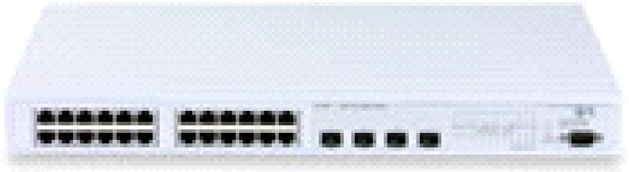


Figure 3.1. 3com Superstack 3 Switch 3824 (3c17400) (From Ref. 46).

3. Network Interface Controller (NIC)

Often abbreviated as *NIC*, it is an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.[15] The NIC is the primary hardware component that allows the end-user access to the wired network via the wireless AP. It comes in different variations. One type of NIC can be installed into the laptop computer by way of a PCMCIA slot on the mother board. The next type is already attached to the motherboard internally. There are other types of NIC cards, but since this paper is discussing healthcare provider mobility it is best to discuss just these two. Figure 3.2 shows some examples of NICs that can be purchased as COTS.

[14] Mitchell, Bradley. Switches. [http://comnetworking.about.com/library/glossary/bldef-switch.htm]. Last accessed July 2004.

[15] Network Interfaces Cards. http://ww.webopedia.com/TERM/n/network_interface_card_NIC.html]. Last accessed July 2004.

Figure 3.2. D-link DWL-650; Dell Trumobile; Linksys Wireless G (From Refs. 47, 48, & 49).

4. Access Points

Access Points are hardware devices or a computer's software application that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to. APs, through software protocol, can prevent unauthorized end-users access to the AP by using the Wired Equivalency Privacy (WEP) protocol, or Wi-Fi Protected Access (WPA). APs provide access via an authorization network protocol, which allows an end-user the ability to communicate with the wired LAN. The software application of the AP can provide MAC filtering that allows only specified MAC addresses authorization to the network. Figure 3.3 shows examples of what an Access Point may look like.

Figure 3.3. Intel Pro Wireless 2011B LAN Enterprise AP Hub; Cisco Aironet 1200 Enterprise AP; HP ProCurve Wireless Enterprise AP (From Refs. 56, 57, & 58).

5. Shielding

A concern for utilizing wireless within an MTF is the interference that may be encountered with other medical equipment. There are different types of wards in an MTF. Each one brings to the table a different situation that may result in the failure of their equipment if an access point were to be installed within close proximity. Studies have shown that using the 802.11 frequency around medical equipment poses little threat to the medical equipment within range of its signal. There is very little evidence that EMI is the cause of fatal accidents within an MTF. This allows APs to be placed in key areas of the MTF and provide wireless access for the health care providers to gain access to the patient information needed.

Currently, the only ban being put into place for EMI management within DoD MTFs is in regard to cell phone use. Most hospitals have bans on the use of cellular phones inside their facilities, despite the absence of any comprehensive scientific information supporting the impression that cell phones are dangerous in hospitals. For years, the FDA and FCC have known that EM radiation from various sources could interfere with delicate medical equipment. The ban on cell phones in hospitals has grown to become one of the "urban myths" of our society. But, there is no such ban. [16]

A report in 1997 from the National Health Service in England, DB9702, stated that only 4% of handheld transmitters (all types) cause any interference at a distance of one meter (~3 feet). Also, the study stated that, "The type of radio handset made a large difference to the likelihood of interference." At a distance of 1 meter, 41% of medical devices suffered interference from emergency services handsets, 35% suffered interference from security/porters handsets but only 4% from cell phones. No significant levels of interference were detected from cordless handsets/local area networks or cellular base stations.[17]

[16] Gilfor, Jeff Dr. Wireless devices and Electromagnetic Interference in Hospitals, Urban Myth? [http://www.pdamd.com/features/interference.xml]. Pg. 1. July 2004.

[17] MDA. MOBILE COMMUNICATIONS: INTERFERENCE WITH MEDICAL DEVICES. [http://www.medical-devices.gov.uk/mda/mdawebsitev2.nsf/0/483b6bb5b6fbc80780256c8b003c88f3/$FILE/sn9706.pdf]. April 1997.

C. NETWORK TOPOLOGIES

1. Multi-Point (Star)

The opportunity to use a Multi-Point (Star) topology may occur when there is a need to broadcast the wired LAN into areas where there may not be an IT infrastructure available. A star topology allows areas within the MTF architecture the opportunity to receive network access from a central point of access. An example of this would be a large hospital that has multiple satellite buildings set up around the main building. Instead of spending a large sum of money to install wires to connect each building a wireless network can be set up to allow network access by using antennas atop each building. This allows each building to receive the network transmission. Once each building has received connectivity through the antenna, then it can be sent throughout the building via CAT 5 cable to each of the APs within and broadcast. Another example is just having an AP fixed within the center of a room or office. This AP would broadcast a 360 degree directional signal to everyone within the vicinity and they may be able to communicate through the AP to one another. Figure 3.4 shows how the multi-point (star) topology works outdoors, while Figure 3.5 demonstrates how the AP inside would broadcast.

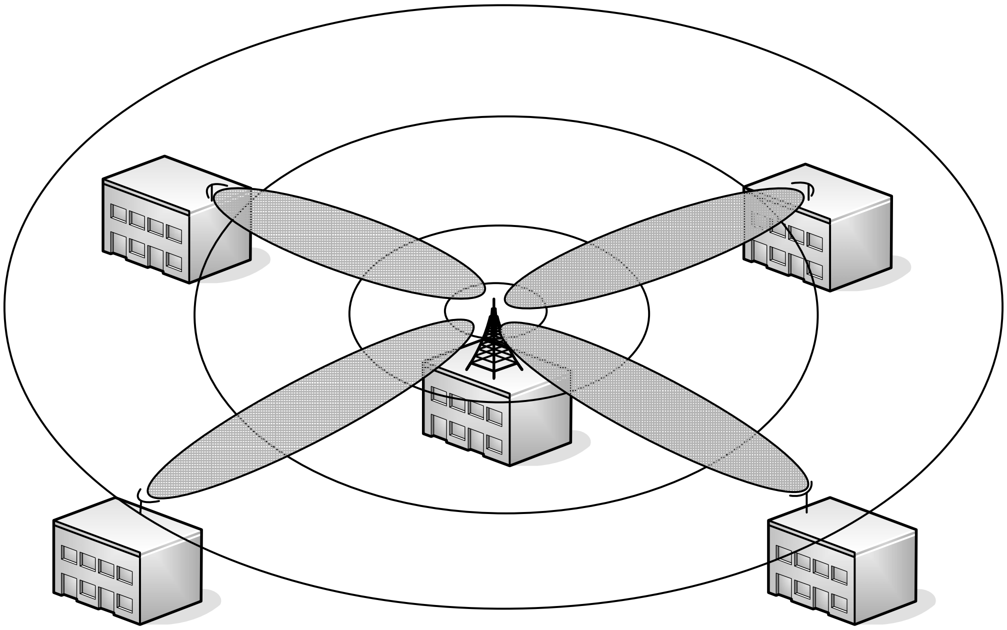


Figure 3.4. Multi-Point (Star) Topology with Omni and Semi-Directional Broadcasts.

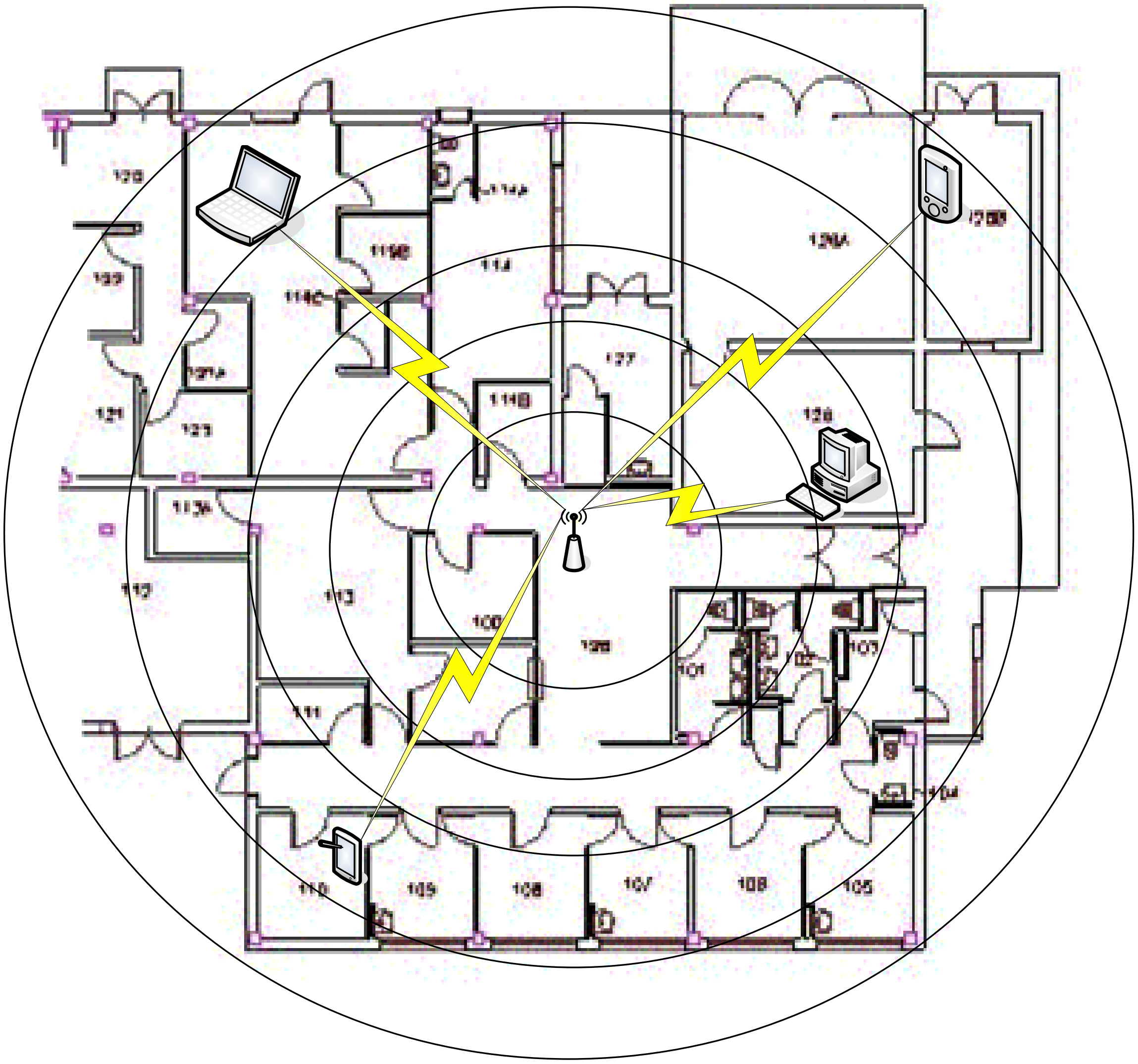


Figure 3.5. Wireless Multi-Point (Star) Topology from AP Inside Building.

2. Point-to-Point

Point-to-Point topology may be used in certain situations where only a key area needs to be transmitted to. If the need arises to create a WLAN that requires the signal to focus its path towards one floor a point-to-point topology may be the trick. The idea would be to adjust the antenna's broadcasting cone toward one end of the building towards the other. Now, with that said, the antenna used my cause some sort of bleed over within its immediate position. Examples of this would be the yagi, patch, or panel antennas. They provide a semi-directional cone, but also bleed off to the sides. Figure 3.6 is a diagram of how yagi and patch panels broadcast. Figure 3.7 is an example of what a point-to-point semi-directional topology would look like outdoors. Figure 3.9 demonstrates the use of a semi-directional antenna indoors.

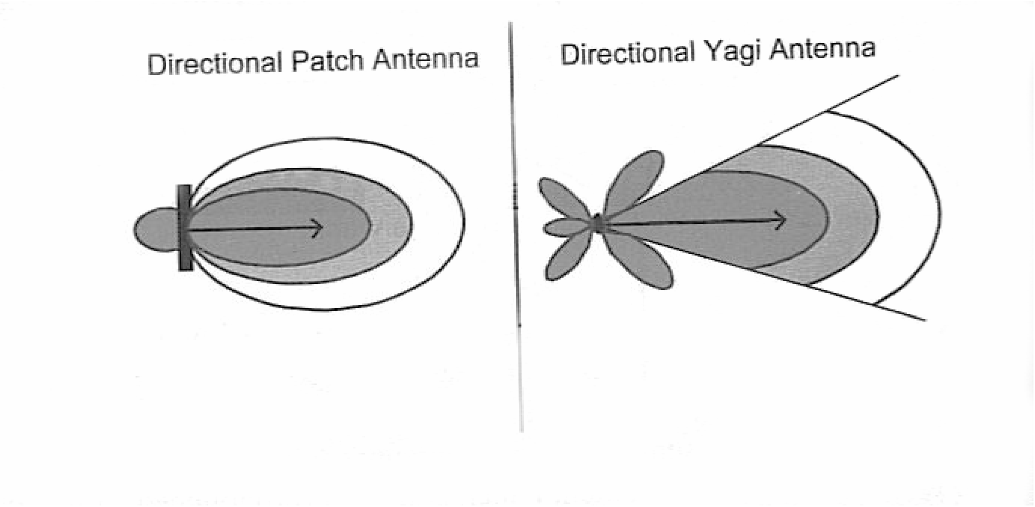


Figure 3.6. Signal Direction for Patch and Yagi Antenna.[18]

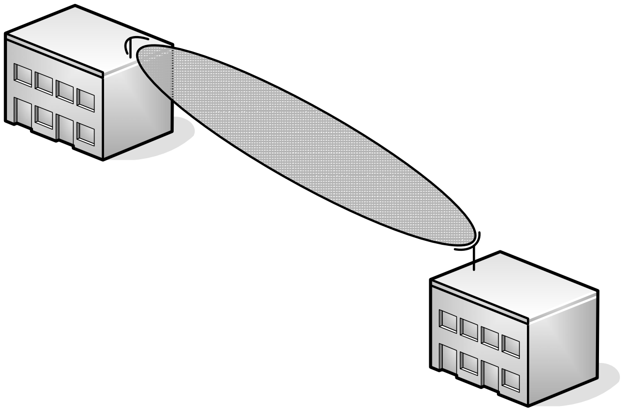


Figure 3.7. Point-To-Point Topology Showing Semi-Direction Broadcasting Outdoors.

[18] Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill. 2003.

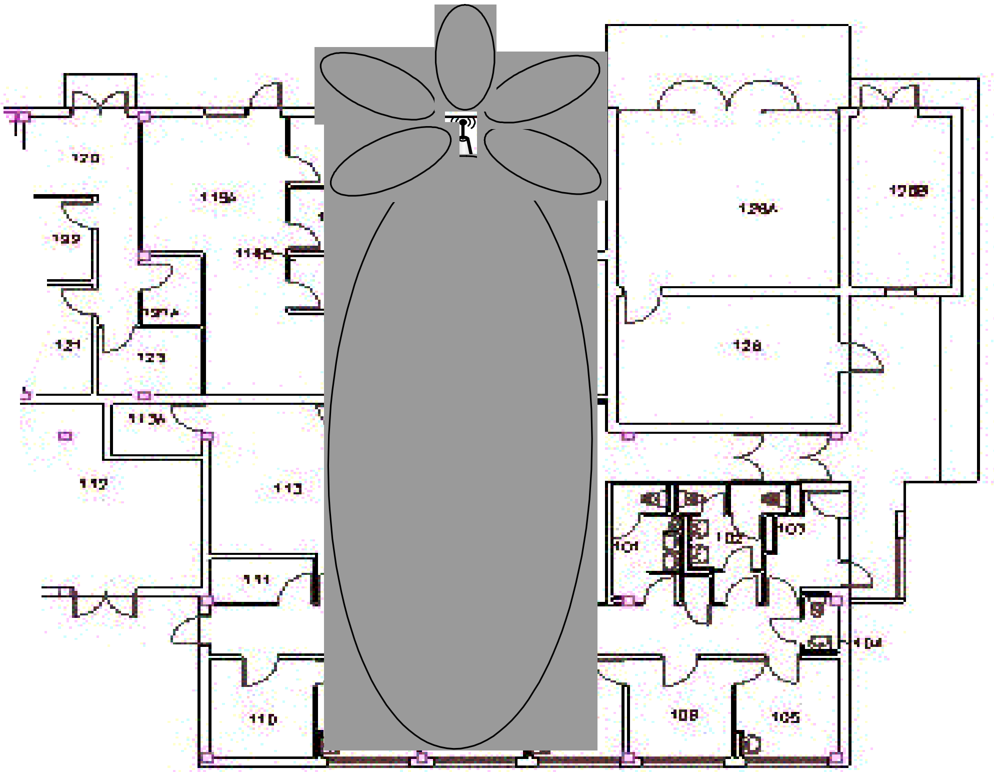


Figure 3.8. Semi-Directional Broadcast Indoors.

D. SECURITY

1. Threat Assessment

During a site survey a need to establish what the threats are is very important. There are different types of security threats that plague wireless. Since the medium used by wireless is broadcasted over the airwaves the ability to pull packets right out of the air is simple. The task for a security manager is to prevent the information floating over these airwaves from being deciphered by unauthorized patrons. There are different types of attacks that a WLAN may encounter. Also, there are different types of attackers. Disgruntled employees that are currently working or were previously employed by the company can perform malicious acts to get back at their employers. Another attacker is the one from the outside. This person could be using the social engineering concept by talking to employees to gather information, or by just browsing the web-sites for discrepancies. They can also just sit outside the target of choice and perform their attack. Outsiders can use both the passive or active attack upon an unsuspecting target.

A passive attack means that the person performing the attack has no intentions of maliciously compromising the network in which it is monitoring. The attack is more like an information gathering exercise. There are different types of software applications that can perform these types of passive attacks.

Passive attacks involve packet capturing. With the right software any person can detect what type of signal is being broadcast. They can tell the SSID, whether or not it is using WEP, and its frequency. Other types can gather the packets that are being transmitted through the air. It may take millions of packets to decipher what the encryption key is for WEP, but it can be done in just a matter of hours or a few days. If the key is greatly encrypted, then it could take a much longer time.

An active attack is designed for the sole purpose of manipulating a network or system depending on the need. An active attack attempts to perform by connecting to the system by backdoor capabilities. Once the system is compromised the ability to probe the network becomes quite easy. Network configurations can be performed to allow the hacker authorization by becoming an end-user through an account that is created.

One active attack is the Denial of Service (DoS). This can also be called jamming. Since it is a radio frequency the opportunity to jam the signal is there. It does not take much to perform this task. An attacker can jam all the radio communications of a WLAN with high powered transceiver. It is almost impossible to protect yourself against such an attack, except perhaps, with some very sophisticated/hard-to-use equipment, like faraday's cage.[19]

An interesting attack is the man-in-the-middle attack. This task is performed by creating an Address Resolution Protocol (ARP) poisoning. This attack allows the hacker the ability to “spoof” the AP Media Access Control (MAC) address, which causes the other MAC addresses associated with the AP to transmit data through the hacker’s MAC

[19] Räty, J. and Kaukinen, S. Defeating security in wireless LANs. Pg. 3. Last accessed July 2004.

address. It is another form of information gathering, but in can be used for malicious activity along the network as well. This could be considered a DoS if the man-in-the-middle decides to manipulate both end-users into thinking that the information received is authentic from the person assumed to be the sender. Therefore, the original information that is expected to be received by the right MAC address is compromised by the hacker and the original information is stopped dead in its tracks and configured however the hacker desires.

2. Tools to Prevent

There are different tools that are available to help deter or prevent an attack from occurring, and many more are being created just as fast as new technology arises. The ones discussed within this paper are the more common applications that help in deterring the common "script kiddy" hacker and possibly the professional "black hat" hacker as well.

a. Wired Equivalency Privacy (WEP)

WEP is an algorithm designed to help encrypt the data that is transmitted over a wireless network. Granted, it is not the cure all for wireless, but it is better than broadcasting important information over the air unprotected. WEP encrypts only the data being transmitted. The disadvantage of that is the header is left in plain site for those who may be gathering packets. As mentioned before the use of WEP has its limitations. WEP's security flaws have been widely known ever since January of 2001, when the University of California at Berkeley issued a highly publicized paper. Since then, WEP has been roundly criticized for flaws that include weak encryption, characterized by keys that are no longer than 40 bits; static encryption keys; and lack of a key distribution method.[20] The ability to crack WEP is becoming much easier. The need for a stronger encryption tool is underway, along with the creation of various IEEE wireless groups focusing on this issue as well.

WEP is an RC4 64-bit stream cipher that the 802.11 committee intended to be used for both authentication and encryption. RC4 is a weak encryption and the

[20] Emigh, J. WPA: Is Wi-Fi's Security Bandage Going to Win Over Network Admins? [http://www.wi-fiplanet.com/tutorials/article.php/1550561]. December 2002.

designers knew this at the time of selection. Existing US encryption export laws restricted more advanced encrypted data algorithms. The 802.11 group felt that capturing foreign markets was more important then security. It was later discovered that there were even more significant flaws in the WEP design.

The most fundamental problem is when WEP is used for authentication. The process begins where the access point generates a random sequence of characters and sends them to a client requesting access to the wireless network. In order for the client to gain access to the network it must encrypt the string and send it as a response. The AP then decrypts the string, and if it matches its original transmission, the client is granted access. The problem with this method is that it allows a would-be hacker the possibility of intercepting both unencrypted challenge and the encrypted response.

A hacker can then easily derive the WEP key from these two values. Secondly, a hacker might also begin a brute force or dictionary attack to derive the WEP key. A brute force attack is to try every combination of keys and a dictionary attack is to try variations of common words. The effectiveness of this attack is that the AP will respond immediately if the WEP key for authentication is correct or not. It is highly recommended that WEP not be used as the only means of authentication. By themselves WEP keys can be hacked in as little as 15 minutes if used for authentication. Bill Arbaugh's paper *Your 802.11 Wireless Network has no Clothes* [21] explains this vulnerability in greater detail. WEP keys are also used for data encryption. Unfortunately the WEP key can be reversed engineered by hackers if approximately 5-10 million packets can be intercepted even if WEP is used solely for encryption and not for authentication. On a heavily loaded network this might take several hours. On a lightly loaded network this traffic analysis might take up to a week. The vulnerability is based on statistical analysis due to the repetition of the initialization vectors. Fluhrer, Mantin, and Shamir's paper *Weakness in the Key Scheduling Algorithm of RC4*[22] and Adam

[21] Arbaugh W. Your 802.11 Wireless Network Has No Clothes. [http://www.drizzle.com/~aboba/IEEE/wireless.pdf]. March 2001.

[22] Fluhrer, Mantin, and Shamir. Weakness in the Key Scheduling Algorithm of RC4 [http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf]. August 2001.

Stubblefield's *Using Fluhrer, Mantin, and Shamir Attack to break WEP*[23] explains this vulnerability in greater depth. Freeware Linux programs AirSnort and WEP Crack can be downloaded at http://airsnort.shmoo.com/ and http://sourceforge.net/projects/wepcrack to crack WEP using a Linux operating system. Lucent, Cisco and several other vendors have upgraded their firmware to prevent the exploitation of this vulnerability when using their cards. Nevertheless, if a hacker can mount an active attack using a non- upgraded firmware card, the WEP vulnerability still exists. Of course the 5-10 million packets of interception can then only work between an access point and a client with a non-upgraded firmware card. This may force a hacker to actively interact with a target network using a non-upgraded card. This would pose greater risk for the hacker because going active might reveal the hacker's position. So it is a good idea to upgrade your firmware so it will take longer for a hacker to crack the WEP key and increase the hacker's visibility**.**

The length of the encryption in the 802.11 spec is 64 bits which includes a 24-bit initialization vector and a 40-bit encryption key. Most vendors have allowed for longer keys such 128-bit and 152-bit keys. They are also referred to 40, 104, and 128 bit keys because of the 24 bit IV is not counted. This has caused confusion, but they are in fact the same. Also according to Jessie Walker's paper *Unsafe at any key size; an analysis of the WEP encapsulation*[24], increasing the WEP key does nothing to increase WEP's resistance to attack because of how WEP uses cryptography, not the key size. Because the 128 and 152 WEP keys sizes are not specified in the 802.11 specification use of multiple vendors can cause interoperability problems. The long-term solution as expressed by the 802.11i group is to replace WEP with Advanced Encryption Standard (AES). In the mean time if no other encryption mechanisms are available, it is recommended to use WEP and upgrade the firmware on all access points and all user clients.[25]

[23] Stubblefield, A. Using Fluhrer, Mantin, and Shamir Attack to Break WEP. [http://www.cs.rice.edu/~astubble/wep]. August 2001.

[24] Walker, J. Unsafe at Any Key Size; An Analysis of the WEP Encapsulation, [http://www.drizzle.com/~aboba/IEEE/0-362.zip]. October 2000.

[25] Roth, Joseph L., Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions. Master's Thesis. Naval Postgraduate School. Pg. 44-46. Monterey, California. September 2002.

b. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access is a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

It should be noted that WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.[26]

c. Virtual Private Network (VPN)

Virtual Private Networks are formats that create "tunnels" within an existing public LAN or WLAN. These tunnels allow information to be transferred over the LAN or WLAN encrypted. They can be defined as encrypted tunnels with access control and host or user authentication. VPNs provide a more active form of security by either encrypting or encapsulating data for transmission through an unsecured network. These two types of security—encryption and encapsulation—form the foundation of virtual private networking. However, both encryption and encapsulation are generic terms that describe a function that can be performed by a myriad of specific technologies.

[26] Internet.com. Webopedia. WPA. [http://www.webopedia.com/TERM/W/WPA.html]. Last accessed July 2004.

To add to the confusion, these two sets of technologies can be combined in different implementation topologies. Thus, VPNs can vary widely from vendor to vendor.[27]

They use encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines, but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or possibly by routers. Link-level (layer 2 and 3) encryption provides extra protection by encrypting all of each datagram except the link-level information. This prevents a listener from obtaining information about network structure. While link-level encryption prevents traffic analysis (a form of attack), it must encrypt/decrypt on every hop and every path. Protocol-level encryption (layer 3 and 4) encryption encrypts protocol data but leaves protocol and link headers clear. While protocol-level encryption requires you to encrypt/decrypt data only once, and it encrypts/decrypts only those sessions that need it, headers are sent as clear text, allowing traffic analysis. Application (layer 5 up) encryption is based on a particular application and requires that the application be modified to incorporate encryption.[28]

An example of how a wireless VPN works can be seen in Figure 3.9. First, the user's computer connects to an access point in the uiuc-wireless-net network and is assigned an IP address in that range (172.21.0.0 /20). Machines on this subnet are not allowed to access anything outside that network without authenticating through the VPN server.

Next, when the user runs the VPN client, the computer makes a VPN connection request which is routed to the VPN server. The router sends VPN connection requests from the uiuc-wireless-net to the VPN server, but drops any requests for other campus locations or the Internet from uiuc-wireless-net.

[27] Virtual Private Networks. [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm#xtocid2]. Last accessed July 2004.

[28] Dictionary.com. VPN. [http://dictionary.reference.com/search?q=virtual+private+network&r=67]. Last accessed July 2004.

The VPN server takes the user's authentication request and communicates with the Radius server and the Kerberos server to determine whether the user is authenticating correctly. If so, the VPN server establishes an encrypted tunnel with the wireless computer over the blue path (using the computer's real ID). The VPN server takes the encrypted communications the client computer sends to it, de-encrypts the information, and forwards the information along to its destination with its identity represented as a part of the VPN-assigned network address range.

Requests from computers in the uiuc-vpn-net address range are allowed access to both campus resources and the Internet. Requests that would not be permitted if the router received them unencrypted from uiuc-wireless-net are permitted after the VPN server has begun representing the computer's identity as part of the uiuc-vpn-net address range. The VPN server is the only machine that knows the blue computer's true identity and location; it exchanges information over the encrypted tunnel it established with that machine, and redirects the data as though it originated in an unencrypted form from a machine with a uiuc-vpn-net IP address.[29]

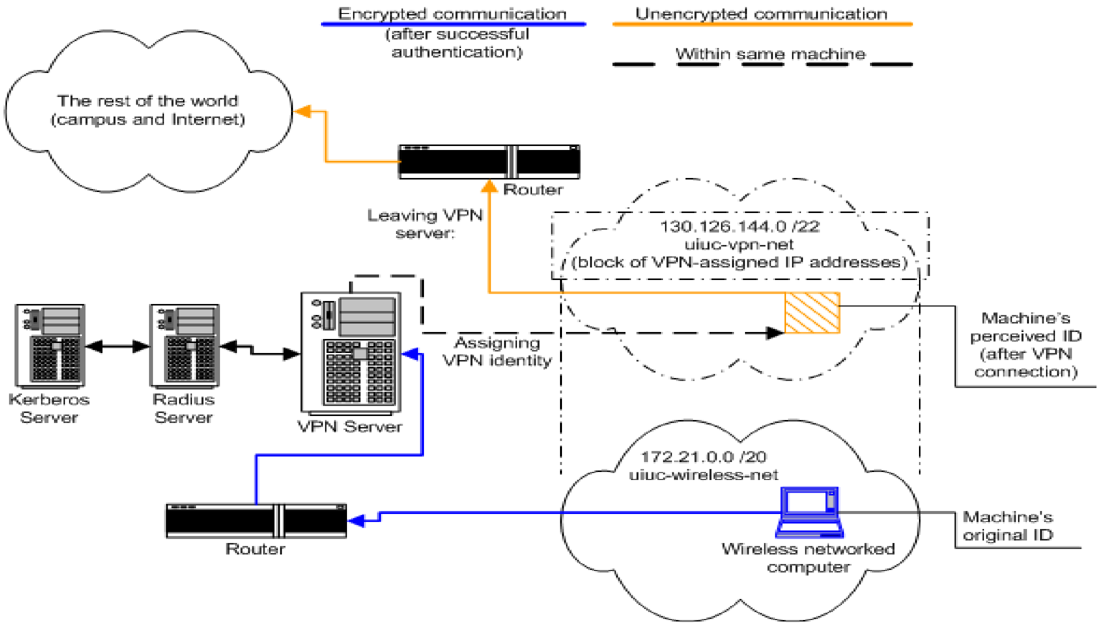


Figure 3.9. Virtual Private Network (From Ref. 29).

[29] Cites. VPN networking diagram. [http://www.cites.uiuc.edu/vpn/vpnnetdiagram.html]. Last accessed July 2004.

d. Secure Shell (SSH)

Secure shell was developed by SSH Communications Security Ltd. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force SSH to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled. When using SSH's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.[30] It was originally designed to replace popular telnet, ftp and UC Berkley UNIX ‘r’ commands with secured encrypted versions. Secure Shell standard has been expanded to perform these crucial tasks securely:

- secure remote access into a computer system
- securely transfer and copy files between systems
- act as a software VPN or tunnel to secure protocols like SMTP, POP, FTP, Telnet, X-windows which are not inherently secure on the TCP/IP wire[31]

This is important to patient care, since the patient’s information would be broadcasted via radio frequency (RF).

e. Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a protocol that provides an encrypted data stream that is bi-directional. This means that the data is encrypted at the sender’s end, and then decrypted at the receiver’s end. Thus, it allows for both the server and client a two-way verification that is not able to be compromised and alter during the transmission.

[30] Internet.com. Webopedia. Secure Shell (SSH). [http://www.webopedia.com/TERM/S/SSH.html]. Last accessed July 2004.

[31] Pragma Systems Inc. Secure Shell (sshd) Server for Windows NT/2000/XP. Pg. 1. August 2001.

SSL is created to work in between the application and network layer (Please refer to the OSI model in Appendix A.). TCP/IP employs no security measures to prevent data sniffing, hijacking or insertion and is unsuitable on its own for connections containing sensitive information. SSL sits in-between high level protocols (such as HTTP or IMAP) and the low-level protocols of TCP over IP providing the needed security for such transactions to take place. It uses TCP/IP on behalf of the higher level protocols and once the correct client/server software is installed can appear transparent.[32] See Figure 3.10 for diagram.

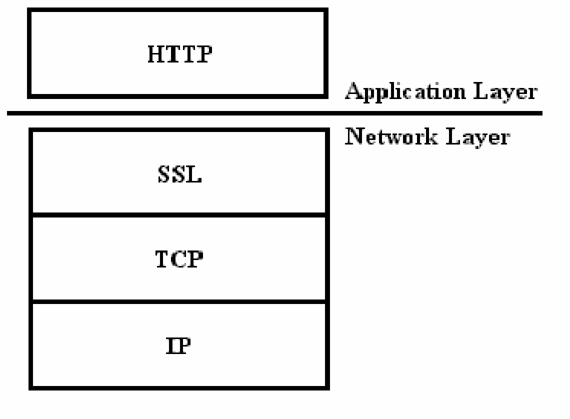


Figure 3.10. Diagram of SSL Operation. (From Ref 50 http://harmony.haxors.com).

f. Intrusion Detection System (IDS)

Intrusion Detection Systems are applications that monitor traffic that enters and leaves a network. They have the capabilities of detecting unauthorized access into the system, as well as determine where they have been throughout the network. There are several ways to categorize an IDS:

- **Misuse detection** vs. **anomaly detection**: in misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection

[32] Fewer, S. SSL. A discussion of the secure socket layer. [http://harmony.hazors.com] Last accessed July 2004.

software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

- **Network-based** vs. **host-based systems**: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
- **Passive system** vs. **reactive system**: in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. Figure 3.11 is an example of an IDS.[33]

[33] Internet.com. Webopedia. Intrusion Detection Systems. http://www.webopedia.com/TERM/I/intrusion_detection_system.html. Last accessed July 2004.

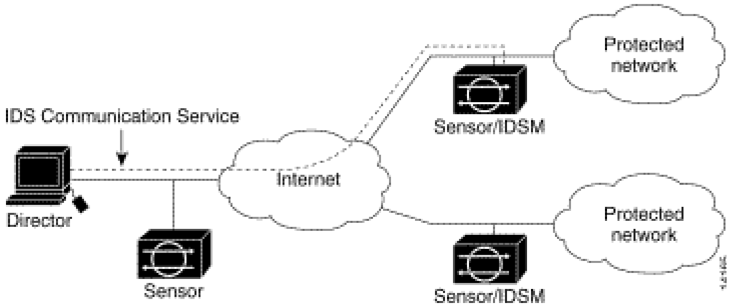


Figure 3.11. IDS Diagram (From Ref. 51).

g. Firewalls

Firewalls are the most common defense for either a LAN or a WLAN. When configured properly they prevent personnel from accessing unauthorized URLs along with the prevention of hackers from entering into the LAN or WLAN. A firewall acts as an interface between the Internet and a private network. It can also be used in an Intranet capacity as well. It regulates traffic between the networks for protecting the internal network from attacks originating from outside the network. A firewall can isolate internal and external traffic by performing a bridge type service. It can make addresses that are internal invisible and not accessible to the outside. The firewall can oversee the facilitation of encrypted connections to external parties over public networks by using a VPN. Firewalls can filter outgoing traffic. They can also filter incoming traffic for malicious data, (e.g. viruses and inappropriate data (pornography), or by external users performing inappropriate actions, such as port scanning. A firewall can block out specific addresses to provide better security and prevent users from viewing unsightly material. Figure 3.12 shows how a firewall can be configured within a network. As seen, there can be multiple firewalls throughout the system. This gives the network more depth to help prevent hackers or other malicious entities from gaining further access.

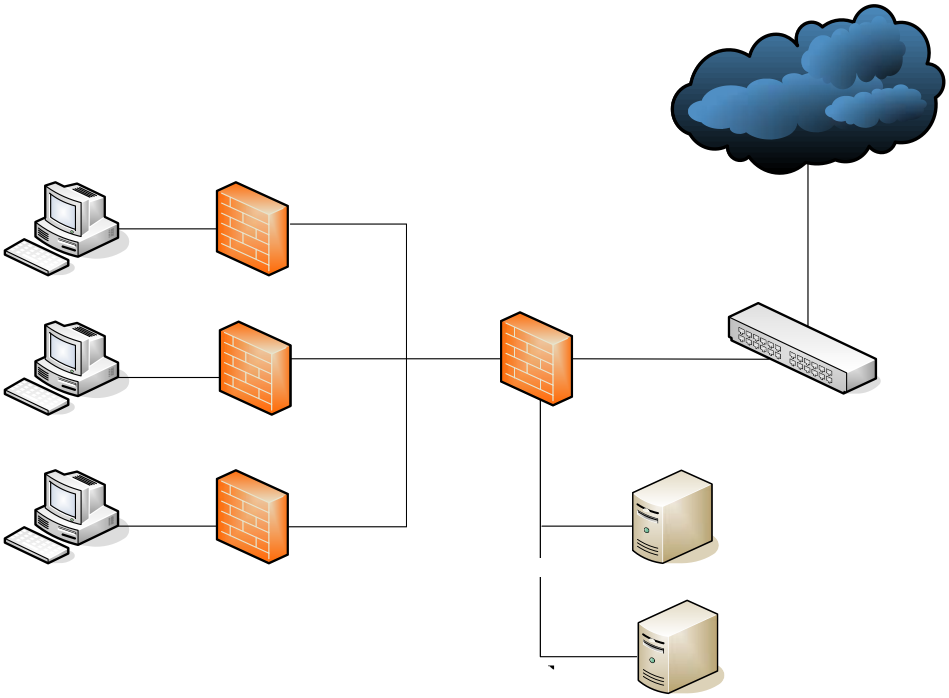


Figure 3.12. Firewall Diagram

E. OTHER RELATED MATERIALS

1. ReefEdge

ReefEdge is a proprietary program that was created to prevent outside activity from entering into a wireless network. It provides an optimized RF environment by monitoring and dynamically adapting APs located in a remote area (e.g. office, building, and a warehouse). ReefEdge has three types of managing tools. The one that can be applicable to this paper is the ReefEdge "Site Manager". It provides comprehensive single site capabilities for centralized authentication, policy, and mobility management. Its provides the following:

- Seamless Mobility

  The Site Manager links all ReefSwitches into a single mobility domain, allowing users to seamlessly roam through the WLAN preserving application connectivity and data security, and eliminating the need to re-authenticate. User sessions are maintained across multiple subnets or

VLANs even when roaming out of wireless LAN coverage, enabling seamless session persistence for mission-critical applications, including VOIP.

- Multi-Layer Security

  A multi-layer security model is implemented and includes authentication, real-time policy management, encryption, and monitoring. Site Manager supports multiple methods of authentication, including device identification, 802.1x, browser-based access, and certificate-based login. Powerful policy management provides fine-grained control over a host of user and device parameters. Site Manager supports military-grade, FIPS-2 certified, IPSec encryption as well as the new WPA and forthcoming 802.11i standards.

- Rapid Wireless Deployment

  Rapid deployment is enabled through Zero-Config technology. Site Manager automatically discovers new ReefEdge WLAN EcoSystem components and deploys them quickly, and effectively. Centralized firmware and configuration management ensures easy maintenance and lower operations cost of the WLAN. Site Manager also supports staging, testing, and automated rollout of software updates.

- IT Integration

  Site Manager integrates the WLAN EcoSystem with existing IT systems, including authentication and policy management servers, accounting and logging servers, and network management systems. Wizards are provided for connecting to RADIUS, LDAP, Microsoft Active Directory, Novell Directory Services, Microsoft Windows domains, Public Key Infrastructure (PKI) systems.

- Site Manager support
  SNMP v1/v2c/v3 with vendor MIBs and traps, as well as custom plugins for HP Openview and CA Unicenter.

- Easy Provisioning of New Applications and Services
  As the WLAN is used for new applications and services; Site Manager takes the guesswork out of deploying these new capabilities. Virtual firewalls are defined around different applications and user types—with each virtual firewall holding a particular access policy, encryption level, and bandwidth allocation.

- Site Manager can be deployed in conjunction with the ReefEdge Air Manager or Multi-Site Manager, components of WiSe OS™. The integrated system GUI provides an overall view of wireless LAN performance and security across clients, access points, and ReefSwitches throughout the enterprise.[34]

2. AirDefense

AirDefense is designed to discover all wireless LAN devices within a network. It provides a network map and inventory, and alerts when devices are unplugged or fail. AirDefense can automatically discover WLAN devices within the coverage of each AirDefense sensor (~40,000–60,000sq.ft.).

AirDefense can provide a real-time depiction of WLAN connections, relations, performance, & usage throughout the network. It is capable of maintaining an inventory of WLAN devices, and alerts to unplugged, stolen, or failing access points if the device has not been seen from the air within a designated period of time. It has many different features. AirDefense provides organizations with detailed information of devices that connect to each other and form ad-hoc networks. It can also detect accidental associations and malicious associations. Another interesting feat is how it can alert the

[34] ReefEdge. Site Manager Software. [http://www.reefedge.com/reefedge/apm.do] Last accessed July 2004.

manager to excessive stations connecting to a single access point and excessive traffic between a single station and an access point and/or the wired network.

A list of AirDefense's wireless security capabilities are as follows:

a. Detection of All Rogue Wireless LAN Devices & Activity

- Access points
- Wife user stations
- Soft Access Points
- Wireless bar code scanners

b. AirDefense Also Identifies Rogue Behavior from:

- Ad hoc networks
- Peer-to-peer networking between user stations
- Accidental associations

c. Analysis of Rogue Connections

- Analyzes all connections made by rogue devices

d. Risk & Damage Assessment

- AirDefense tracks all rogue communication and provides forensic information to identify:
- When the rogue first appeared
- How much data was exchanged
- The direction of traffic

e. Intrusion Detection

AirDefense utilizes its 24x7, real-time monitoring of 802.11a/b/g protocols for the most advanced intrusion detection for wireless LANs. With stateful monitoring of all WLAN attack signatures, protocol analysis, statistical anomaly, and policy violations, AirDefense can identify:

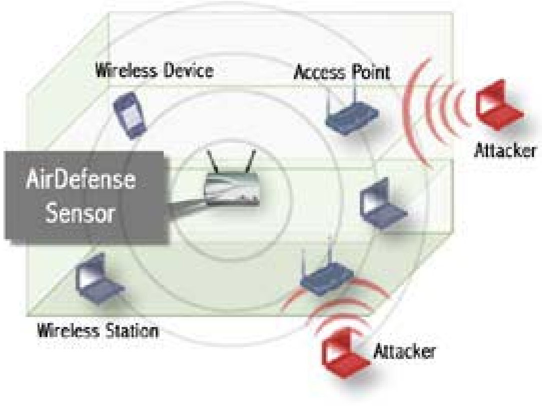


Figure 3.13. AirDefense Sensor. (From Ref. 35).

(1) Attacks Against Wireless LANs. AirDefense correlates data across all sensors to identify attacks in recognized classifications and reduces false positives.

AirDefense recognizes documented and undocumented attacks including:

- Identity thefts from MAC spoofing
- Man-in-the-Middle attacks
- Denial-of-Service Attacks
- Denial-of-Service Attacks with Excessive MAC addresses
- Dictionary attacks

(2) Suspicious Activity & Impending Threats. AirDefense correlates information from all sensors over time to identify suspicious activity, such as:

- Watch list stations/laptops entering the air space;
- Repeated attempts by a station to connect with multiple APs
- Anomalous traffic from unusual off-hours activity or large downloads[35]

[35] AirDefense. Features. [http://www.airdefense.net/products/features/security.html]. Pg. 2-3. July 2004.

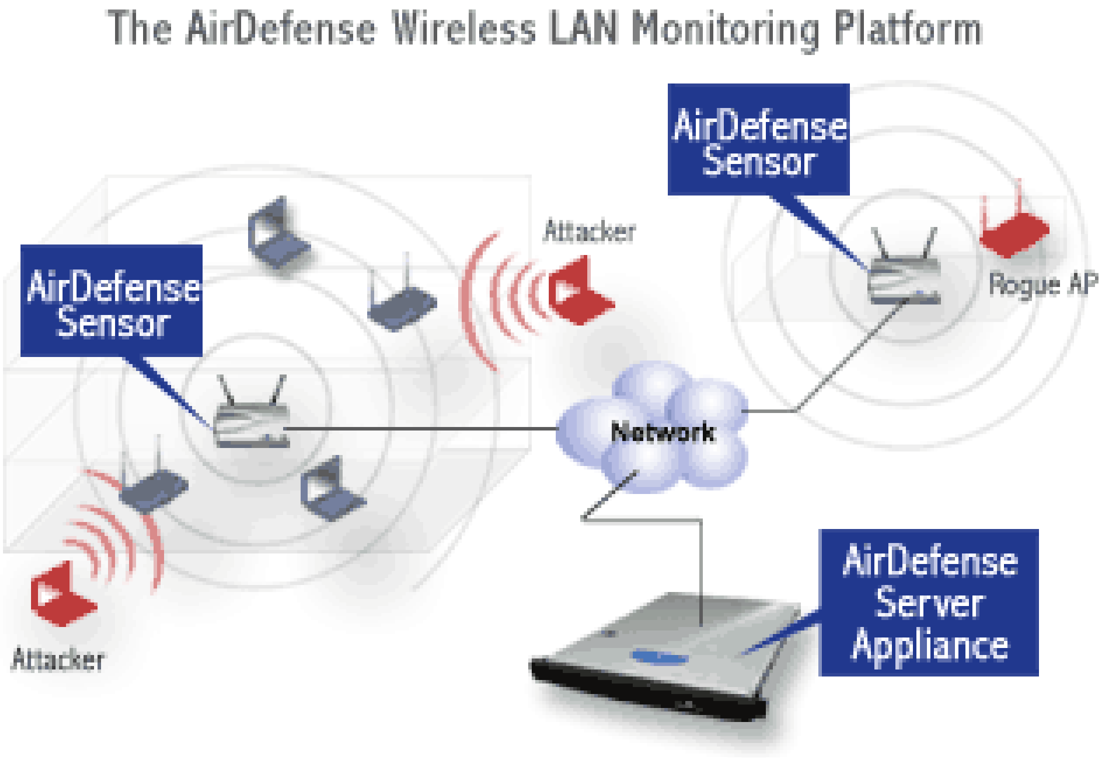

The AirDefense Wireless LAN Monitoring Platform
AirDefense Sensor
Attacker
Rogue AP
AirDefense Sensor
Network
AirDefense Server Appliance
Attacker

Figure 3.14. AirDefense Diagram.[36]

F. SUMMARY

By reviewing the equipment involved, along with the strengths and weaknesses with the software, it is possible to implement a WLAN into an MTF setting. There are more security enhances being created to help prevent the theft of personal identification and other sensitive information from falling into the wrong hands. Instituting the previous mentioned hardware and software can provide for a successful WLAN implementation.

[36] Geroski, R. TechRepublic.com. AirDefense. Diagram. [http://techrepublic.com.com/5100-6264-1059473.html]. Pg. 1. August 2001.

IV. NAVAL MTF WLAN IMPLEMENTATION PLAN

A. INTRODUCTION

A finding within the research of this paper showed an interesting model that could be used to help in the decision making process for implementing a WLAN. A new approach to strategic management was developed in the early 1990's by Drs. Robert Kaplan (Harvard Business School http://www.hbs.harvard.edu) and David Norton (Balanced Scorecard Collaborative http://www.bscol.com). They named this system the 'balanced scorecard'. The Supportability, Usability, and Security (SUS) Model developed by LCDR Joe Roth in his thesis is based as an extension of this framework to help bring order and strategy to the decision making criteria and to derive a successful wireless design and implementation. Figure 3.15 shows the interlocking trinity of the model.[37]

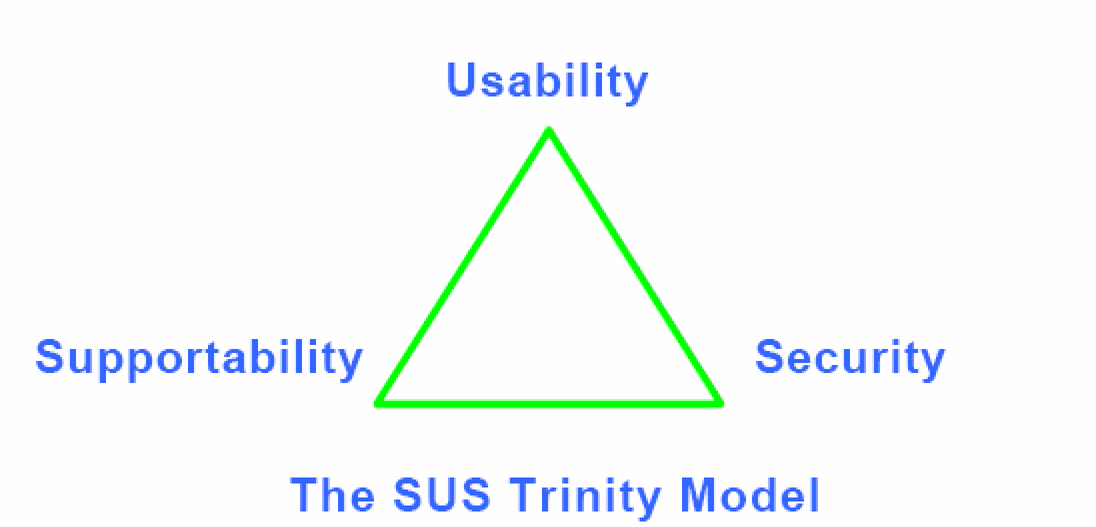


Figure 3.15. SUS Trinity Model (From Ref. 37).

The three entities that make up the model provide the areas of focus when determining what is required by a WLAN in a decision making scenario. Usability is the most important of the three. The reason for this is because if the end user is not able to receive a continuous connection throughout the area of operation then there is no use in

[37] Roth, Joseph L., Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions. Master’s Thesis. Naval Postgraduate School. Monterey, California. Pg. 69. September 2002.

having it installed. It is the whole reason the system would be put into place. Supportability looks not into only provided trouble call support, but the maintenance and training of the WLAN by network personnel and end users is just as important and should not be overlooked. As mentioned before, the basic security default of the WLAN is not the strongest. Therefore, the system is dependent upon multiple layers of security that allow for it to operate on a larger scale throughout an MTF.

B. IMPLEMENTATION PLAN

1. Mission

Navy Medicine, acting as a leading entity amongst DoD medicine will deploy and maintain an industry standard wireless network throughout its MTF facilities in order to provide quality patient care in this critical enabling technology.

2. Assumptions

To complete a requirement analysis, the following assumptions need to be made:

- Wireless technology will be supported by present and future technology.
- Connectivity via wireless is worth pursuing.
- Costs for wireless can be maintained at a controllable level.
- Security aspects and other related issues will have technical solutions to ensure that the wireless network is a valid network.
- The acceptance of wireless technology by the users will happen once it is made available.

3. Stakeholders

a. Executive Leadership

Based on the structure of the military MTF. It is important to place emphasis on the Executive Steering Committees (ESC) of each MTF. This group of individuals will determine the direction of their respective command and maintain overall responsibility for the apportionment and expenditure of allocated funds. The ESC's goal is to make decisions that focus on delivering the best patient care to the Fleet, while maintaining costs. ESCs may not necessarily have the experience with wireless technology, but they may be persuaded to pursue wireless if it will help them achieve their mission goals.

b. Health Care Providers

Health Care Providers are the focus behind the decision to implement wireless into Navy Medicine. They have influence with executive leadership, can make suggestions, sit on committees, etc. This group will be on the forefront when using the wireless technology. They will be able to perform many of their tasks while remaining mobile. Some may have had experience using wireless technology within their private practice prior to joining the military. This group will create the basis of the needs requirements for future wireless applications throughout each MTF based on their medical area of expertise.

c. Administrators

Administrators form another group of people within the MTF that can provide important feedback to the ESC in regards to wireless. This could be considered the middle management of the MTF. They offer another view of how wireless could be implemented on the administrative level. This area of focus is based more on the maintenance of patient data (e.g. records, bills, etc.).

d. Network Managers

Network managers are responsible for the overall effectiveness and security of the network operation. This group is the most technically savvy of all stakeholders. They can see the value of wireless, and make it a goal of the proposed future network. Network managers are generally in favor of new and innovative ideas, and wireless is one of those.

e. External Stakeholders

In the wireless domain, industry is a stakeholder.[38] Navy Medicine will not be developing or buying any Government Off-The-Shelf (GOTS) solutions towards wireless, therefore, it is dependent upon the market. External stakeholders that are involved are regulatory agencies which Navy Medicine must be in compliance with.

[38] Roth, Joseph L., Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions. Master's Thesis. Naval Postgraduate School. Monterey, California. Pg. 78. September 2002.

f. Staff

The staff are the group of users responsible for carrying out the day to day operations of the MTF. They are experts in their respected fields, and can benefit from the wireless technology provided throughout the MTF.

4. Requirements

The requirements for the use of a wireless network are as follows:

a. Mobility

Many of the MTFs have effective wired networks. Wireless networks will piggy back off of the original wired network, which will allow more users access to resources without being fixed in one location.

b. Accessibility

A wireless network will provide access to areas that were considered unavailable due to physical standards. This is a more affordable solution to renovating an area with cables and possible physical alterations to the walls, ceiling, etc.

c. Availability

As mentioned with mobility, the addition of a wireless network will increase the networks availability by helping to reduce in the loss of connectivity.

d. Bandwidth

It is important to have a considerable amount of bandwidth when working with medical operations. With a larger the amount of bandwidth, the greater the capacity to perform radiology and other medical department functions via a mobile PC. 802.11x does not share the same amount of bandwidth as a wired network, but as technology develops the ability to increase the bandwidth wirelessly improves.

e. Ease of Use

A wireless network offers usability without the need for bulky equipment.

C. REQUIREMENTS MATRIX

1. Location

The idea behind this paper is to provide a basic guide, or template, for all Naval MTFs to integrate a wireless network into their current network architecture. Each facility is different then the next, thus a generic template must be created. Areas that may be involved are the main hospital or clinic, along with the outlying supply or other satellite buildings that support the main building. The locations encapsulate the overall end user population of each MTF in which the system is intended for. Table 2 provides an overview of what is required within the network matrix.

Geographic Coverage	The wireless system shall cover the entirety of the main building that represents the Naval MTF, and provide an agile/evolvable capability to allow for the inclusion of its satellite buildings if needed.
Hardware/Software	Systems that are chosen for the implementation/integration should be proprietary products. They shall be interoperable, and conform to wireless industry standards, along with DoD policies and directives.
Availability	Access points that are placed throughout the MTF shall overlap approximately 50% with one another to provide a 99.9% availability.
Security	All equipment shall use WEP, WPA, and other forms of security tools and measures that comply with all specified directives and policies that apply.
Quality of Service (QOS)	The goal of QOS will be to provide 100% service to all end users that depend upon its ability to provide mobility throughout day to day operations.
Bandwidth, Latency, and Packet Loss	Each MTF will have to explore on its own requirements to determine what will be

	require to ensure Quality of Service (QOS) and Service Level Agreements. An example of how it should be presented is as follows: (During peak hours, data rates shall maintain a minimum rate of 56 Kbps regardless of data type or format. Network capacity shall support no less than 25% of the current population of personnel working at that MTF prior to performance degradation. System latency shall be no more than 70 – 100 msecs, while packet loss will be limited to no more than .5%.)
Scalability	Each system chosen should be scalable enough to meet the requirements of the greatest capacity each MTF may provide personnel wise. Provisions should be made for the future implementation/integration of satellite buildings.

Table 2. Requirements Matrix.

2. Hardware/Software

The system designed will be intended to provide wireless access to end users throughout the MTF. Do to the nature of an MTF it would be beneficial to use proprietary hardware and software to ensure that bugs or the possibility of non-interoperability does not occur. The appropriation of access points must rely on the ability to use proprietary, enterprise designed APs as well. The differences between the typical Small Office/Home Office (SOHO) AP and the enterprise version are price and end user capacity. SOHOs are cheaper in cost, and may seem to be more cost effective, but they cannot support large numbers of simultaneous users, provide management software to interact with other APs, or provide a more secure functionality. Savings would not last long, and costs would reoccur more frequently providing more difficulty in configuring, security, and end user satisfaction. By using a proprietary enterprise access point vendor the ability to control all their APs from a single web interface, as well as perform security patches and upgrades, would allow the network to perform more smoothly.

D. COST BENEFITS

The bottom line is still the dollar. Whether it is in the form of reducing the amount of hardware, or increasing provider output, the benefit of deploying a WLAN is still measured quantitatively. When looking at the amount of time saved by allowing the health care provider to see their patients it is obvious that wireless can play an important role in health care. By reviewing the metrics of a health care provider, one would be able to forecast an expected larger percentage of patients seen due to the lack of down time used when inputting data into the system via a stationary position (e.g. desktop PC).

The idea of reducing costs is also evident when the reduction of installing cable and drop boxes throughout the facility are reduced. On average the cost for installing a drop box can range from $75 to $200 depending on location and vendor. The following information provided by recent studies help in determining whether or not it is beneficial to use wireless.

1. Wireless Can Enhance the Return on Investment for Naval MTFs

Another benefit is the real-time application that is provided by allowing the health care provider the ability to perform patient care on a continuous basis throughout their shift. Placing the power of the new enterprise systems into the hands of the medical staff without disrupting the natural process of care will produce many dividends. First of, the attraction of wireless mobile computing will accelerate the adoption of the new systems by clinicians. Wireless will help the staff to accomplish more tasks in a shorter amount of time, to remove redundant process steps, and to increase the accuracy and immediacy of the patient and clinical information that's captured and communicated. The resulting increase in productivity and decrease in errors will help to lighten workloads that are too high now, to increase the quality of patient safety and care, and to accelerate and magnify the return on investment (ROI) of the new enterprise systems.

2. Wireless LAN Benefits Study by NOP World-Technology and Cisco Systems

Cisco Systems and NOP World-Technology studied over 400 organizations in a variety of industries including healthcare[39]. In terms of an ROI on productivity alone, this study found that wireless LAN (WLAN) use in healthcare was responsible for a savings of over $17,000 per employee per year. In surveying end users for wireless LANs in healthcare, this study found that the most cited benefits included flexibility (anytime, anywhere access), mobility (within the building or campus), time savings, and error reduction. They go on to report that users in healthcare stated that they are "almost 50 % more accurate in their everyday tasks."[40] Figures 15 through 25 identify the key areas for determining wireless usage for MTFs. Even though there appears to be quite a few figures, it is important to notice how each of these figures provides key information as to where wireless is moving, along with who is benefiting from its use.

Figure 4.1 shows the overall penetration of WLANs into various areas of industry, education, and government. Healthcare/Medical is still breaking through the barriers.

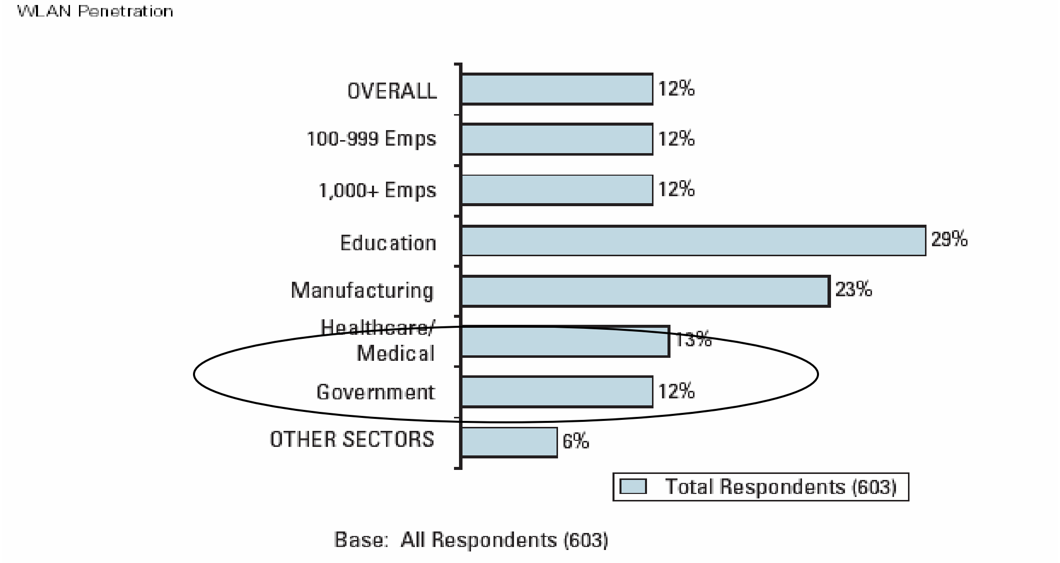


Figure 4.1. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

[39] 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems. [http://www.cisco.com/application/pdf/en/us/guest/products/ps4570/c1031/cdccont_0900aecd800cf91f.pdf]. November 2003.

[40] NETEAM. Making a Case for Wireless Technology in Patient Safety. Pg. 7. March 2004.

Figure 4.2 shows what proportion of employees in each specific area has access to a WLAN. It also shows future projections of that accessibility. By 2005 approximately fifty percent of healthcare will be implementing some sort of wireless network within its own infrastructure.

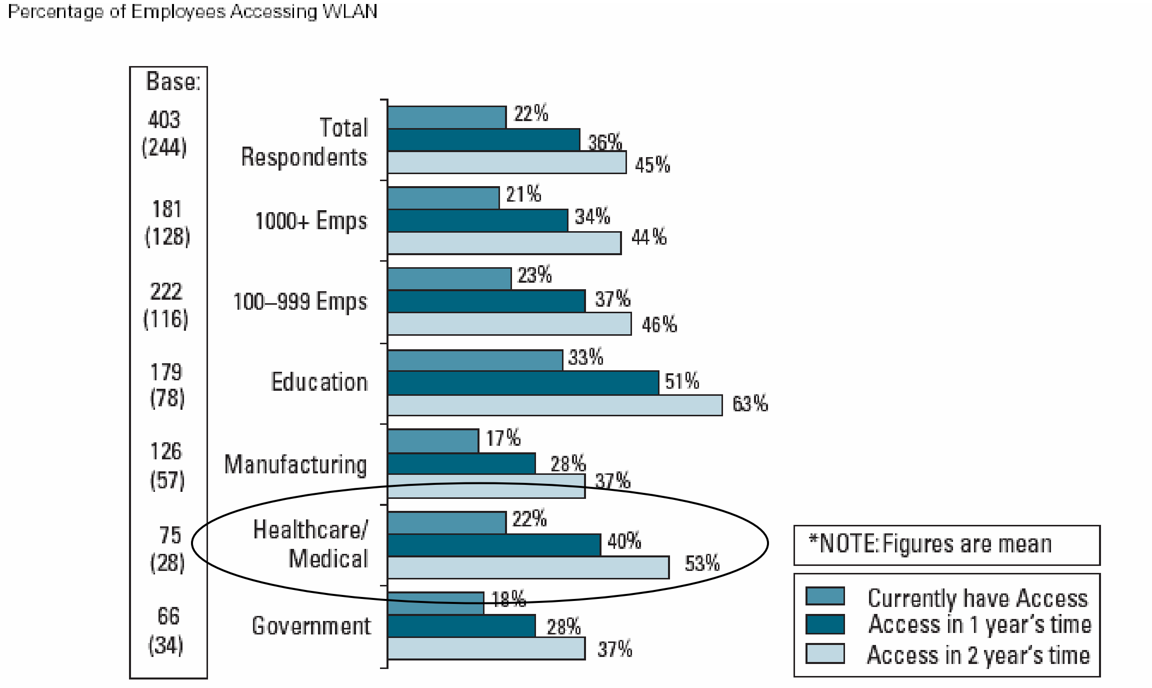
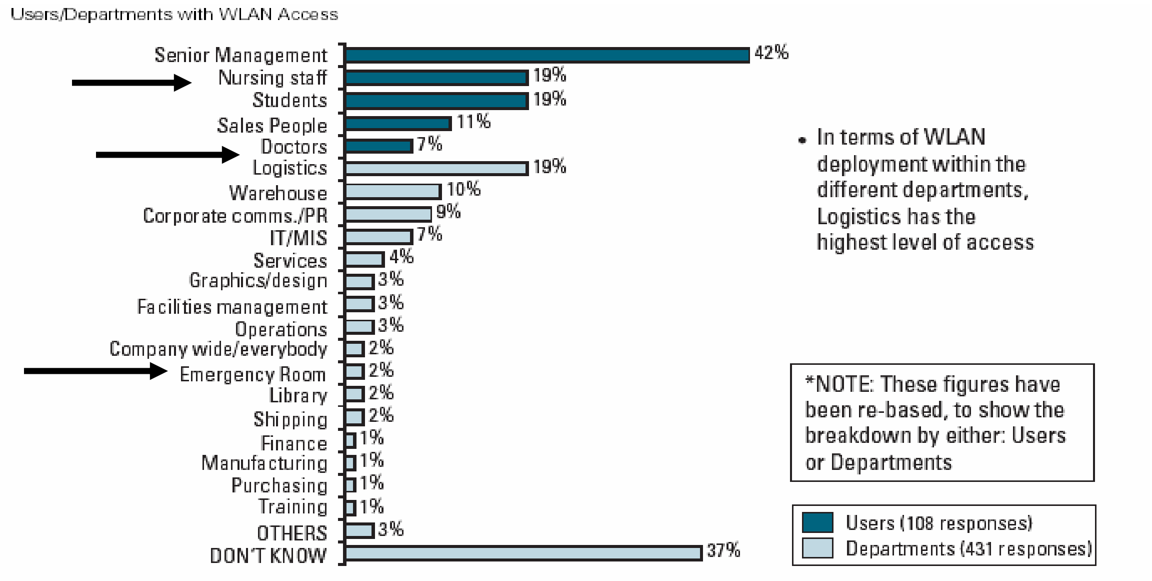


Figure 4.2. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

Figure 4.3 shows who has access to these WLANs. Notice how 'Nursing Staff' has a larger percentage of accessibility than do doctors or emergency personnel.

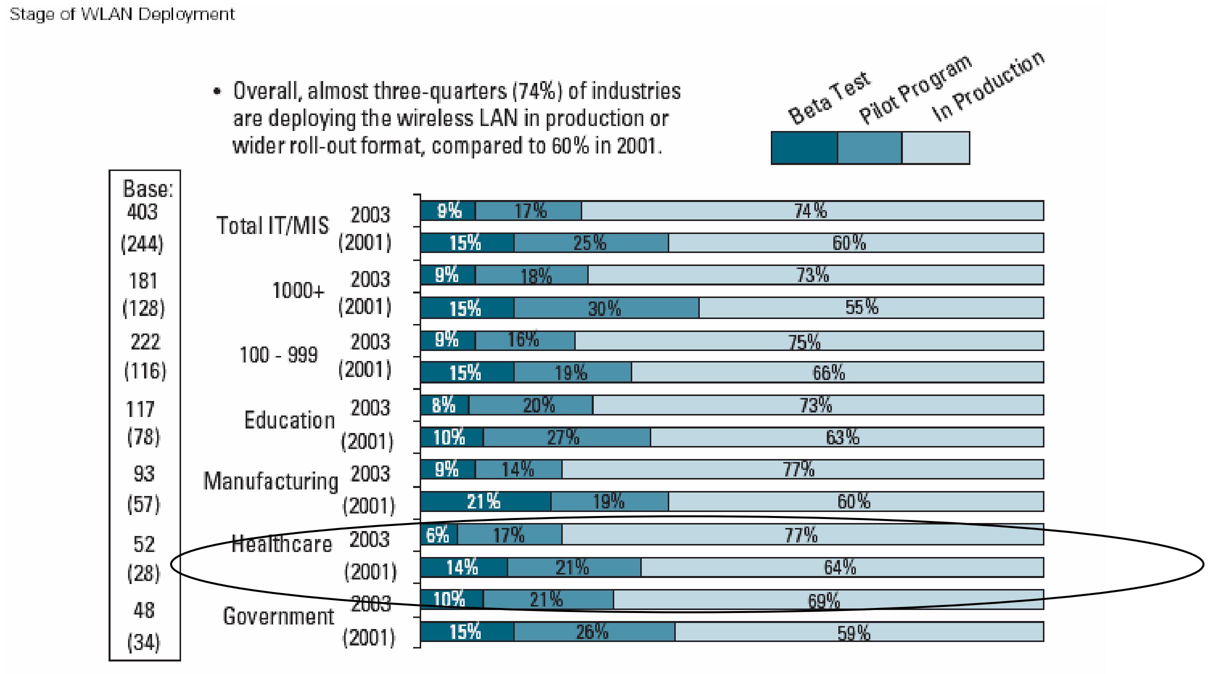


- In terms of WLAN deployment within the different departments, Logistics has the highest level of access

*NOTE: These figures have been re-based, to show the breakdown by either: Users or Departments

Figure 4.3. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

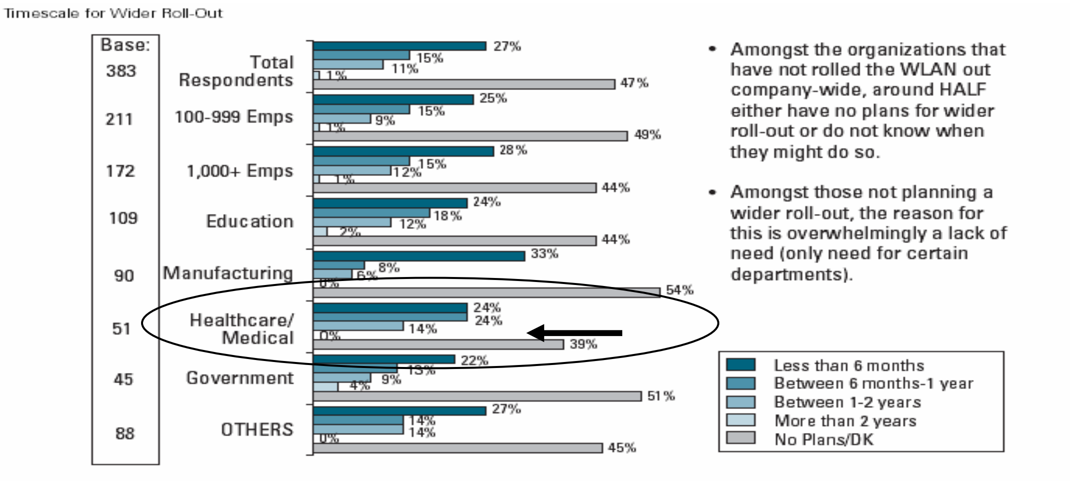
Figure 4.4 shows how healthcare is placing WLANs into production at a greater capacity then previously. By 2005 more than eighty percent of the healthcare entities studied will be utilizing a working WLAN.



- Overall, almost three-quarters (74%) of industries are deploying the wireless LAN in production or wider roll-out format, compared to 60% in 2001.

Figure 4.4. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

Figure 4.5 shows the time table used to predict when the average roll-out will be for each industry. Over fifty percent of the healthcare entities studied plan to roll out a working WLAN within the next year.



- Amongst the organizations that have not rolled the WLAN out company-wide, around HALF either have no plans for wider roll-out or do not know when they might do so.
- Amongst those not planning a wider roll-out, the reason for this is overwhelmingly a lack of need (only need for certain departments).

Figure 4.5. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

Figure 4.6 shows the mean time hours for extended connection use per employee using WLAN. Notice that between government and healthcare entities the hours of connectivity have increased fastest.

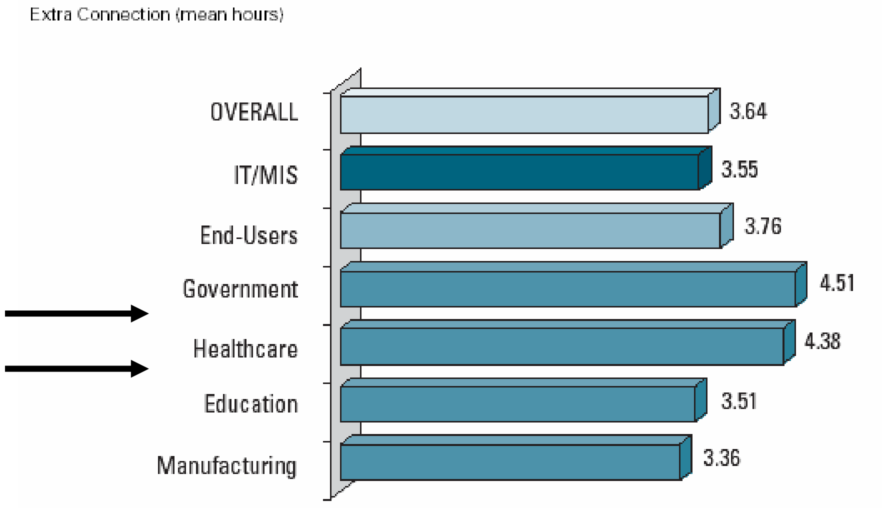


Figure 4.6. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

Figure 4.7 shows the how much time has been saved since implementing a WLAN in each industrial area. According to this study healthcare is the greatest benefactor of this savings.

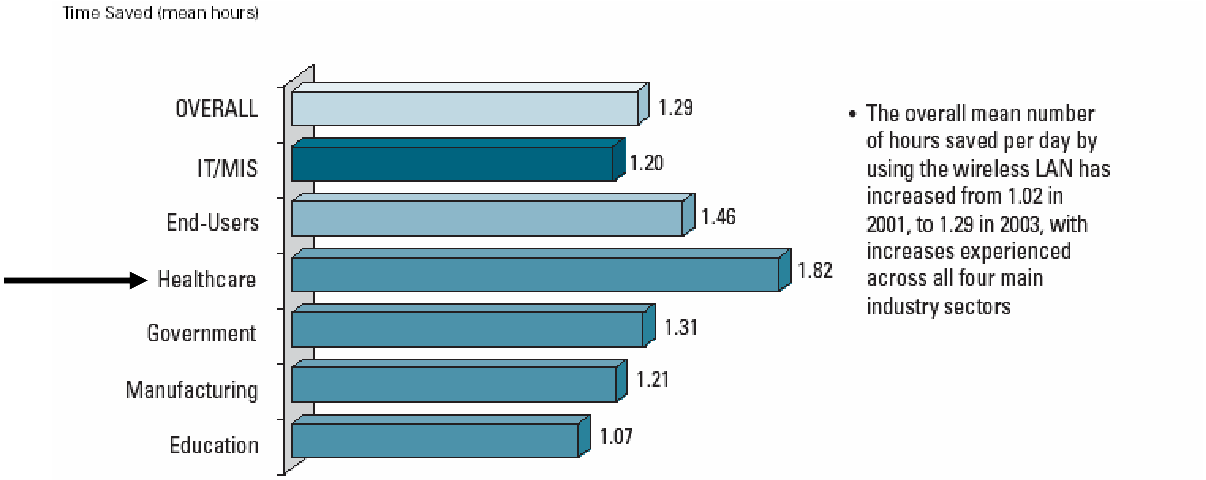


Figure 4.7. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

As mentioned before, the annual cost savings per employee using wireless is quite noticeable. The most noticeable savings in Figure 4.8 is in the healthcare/medical realm.

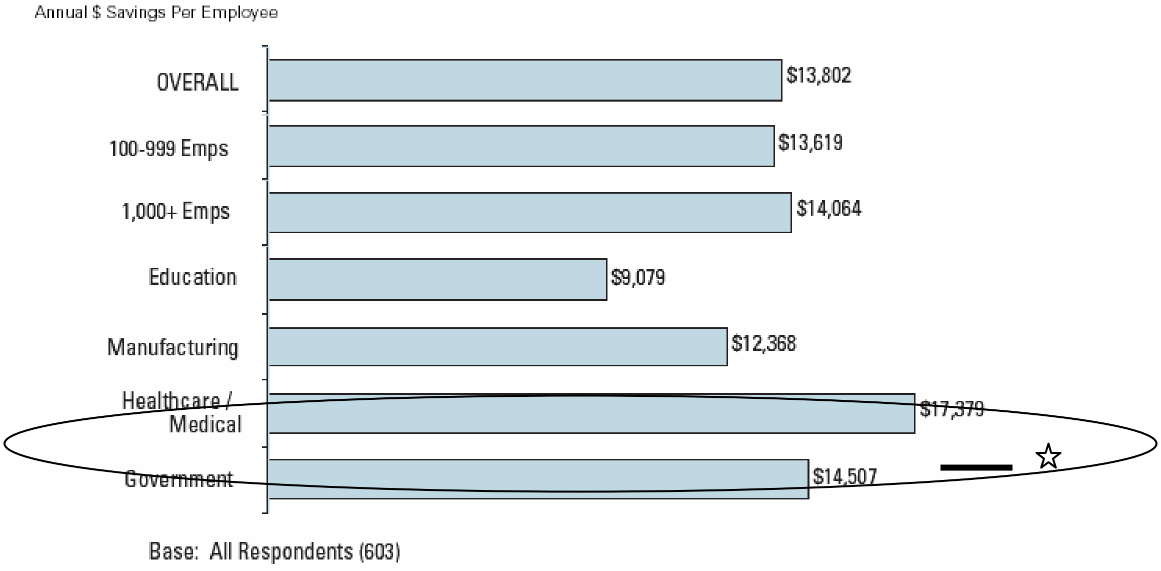


Figure 4.8. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

Figure 4.9 shows that by using a WLAN healthcare productivity has increased by almost a third within the past couple of years.

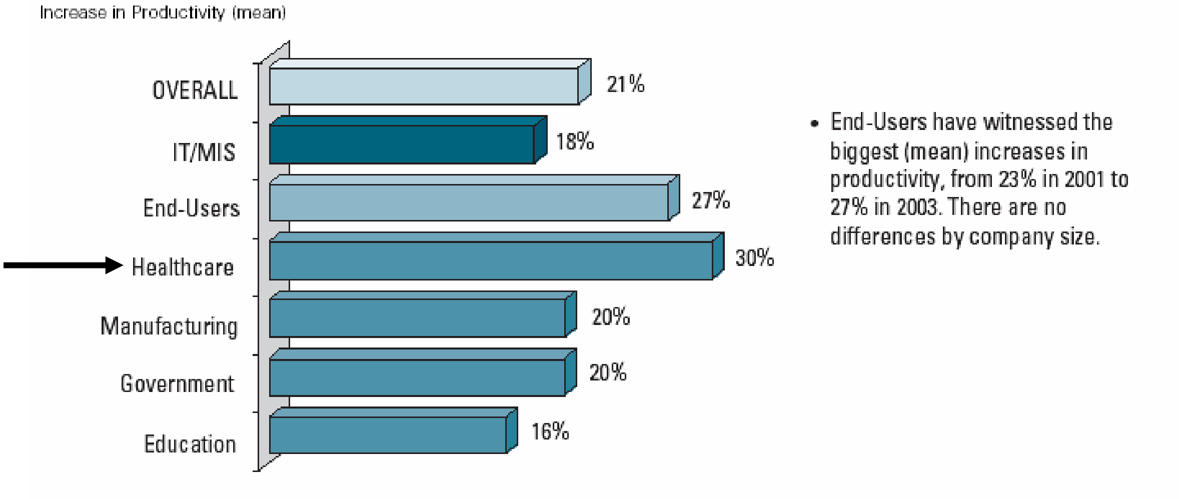


Figure 4.9. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

In Figure 4.10, out of all the healthcare entities studied, forty-three percent of them experienced a significant improvement in accuracy.

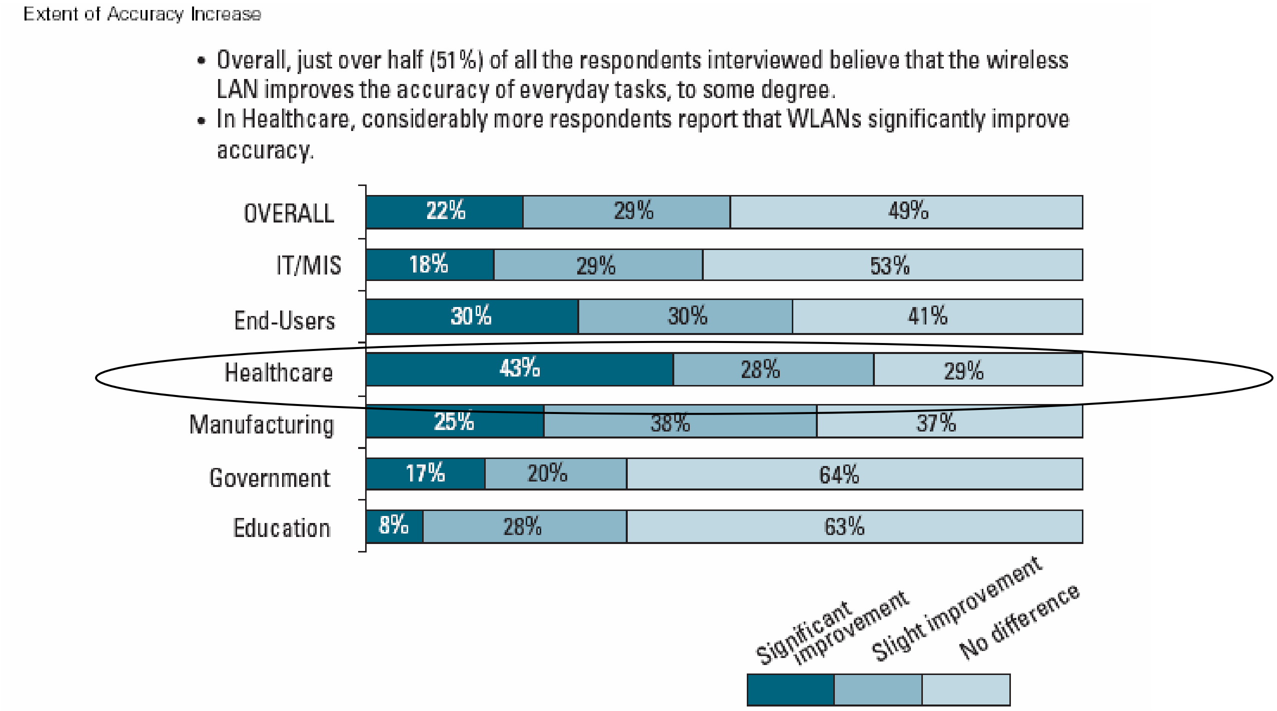


Figure 4.10. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

Last, Figure 4.11 shows that throughout healthcare an increase in accuracy of fifty percent. This is quite a significant increase to the welfare and safety of the patient.

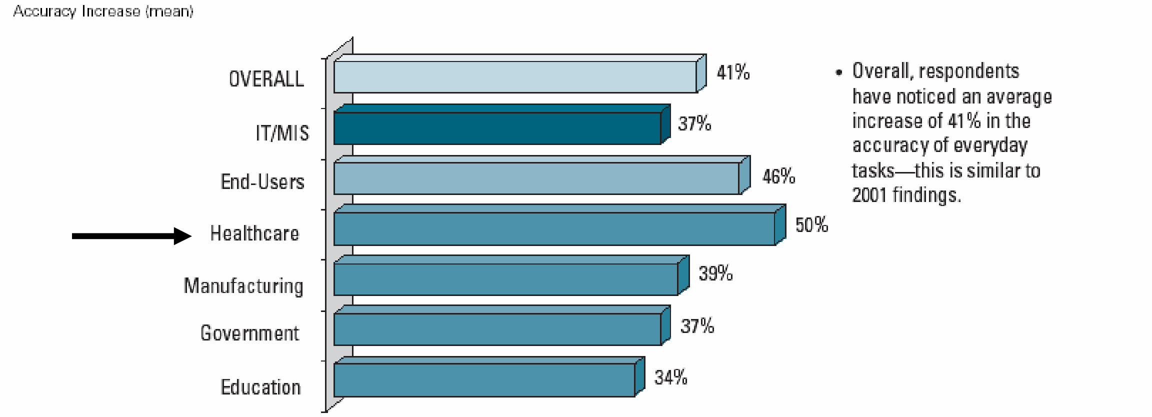
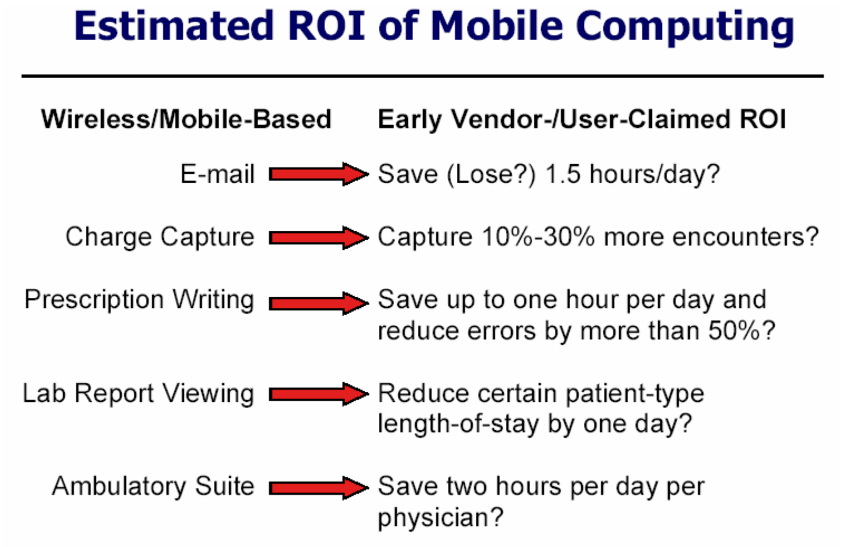


Figure 4.11. 2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems (After Ref. 54).

3. Gartner Group Estimates of Wireless LAN ROI

Kenneth A. Kleinberg, a vice president and research director for Gartner Group, made a presentation at the 2003 Annual HIMSS Conference and Exhibition that stated estimated ROI figures for mobile computing in healthcare[41] (see Table 3 below).



Estimated ROI of Mobile Computing

Wireless/Mobile-Based	Early Vendor-/User-Claimed ROI
E-mail	Save (Lose?) 1.5 hours/day?
Charge Capture	Capture 10%-30% more encounters?
Prescription Writing	Save up to one hour per day and reduce errors by more than 50%?
Lab Report Viewing	Reduce certain patient-type length-of-stay by one day?
Ambulatory Suite	Save two hours per day per physician?

Table 3. Gartner ROI for Wireless/Mobile Computing in Healthcare. [42]

4. Wireless LAN Association (WLANA)

The Wireless LAN Association (WLANA) submitted a report that discussed the benefits of implementing a WLAN. The following information is derived from their report.

a. Major Findings

This Wireless LAN Cost of Ownership report is focused on the results of a detailed end-user survey to identify cost of ownership and tangible and intangible gains in using wireless LAN technology. It is apparent that the technology is taking its place as a viable alternative and/or complement to wired LANs and for new strategic applications.

- 89% of the companies experienced a successful implementation.

[41] NETEAM. Making a Case for Wireless Technology in Patient Safety. Pg. 7. March 2004.

[42] Kleinberg, K. Mobile Healthcare: Applications, Vendors and Adoption. [http://www.himss.org/content/files/proceedings/2003/Sessions/session102_slides.pdf]. Last accessed July 2004.

- 92% of respondents interviewed believe there is a definite economic and business benefit after installation.
- 92% of respondents reported that they will continue to deploy wireless technology in their network through 2000 because of the benefits experienced by end users and/or IT staff.
- Payback was less than one year, across all industries surveyed.

The survey combines both telephone and written responses from 34 organizations. The survey consisted of both open-ended and multiple-choice questions. It was designed to provide the Wireless LAN Alliance (WLANA) with as broad a response base as possible regarding specific costs, attitudes and experiences with their overall wireless LAN ownership. All of the respondents involved subsequently completed a more extensive, follow-up written survey. Companies, schools, and medical facilities were assured anonymity. The analysis that follows identifies only by industry category and reports the data in the mean.

Some important findings are listed below:

b. Real-Time Access to Information

One of the consistent findings of this study was how end-users benefited from real-time information. In fact, 97% of respondents said they either strongly agree or agree that the wireless LAN contributed to the speed in which they completed a task requiring real-time or near real-time access to information.

c. Cost of Ownership

The study compared the costs of 34 wireless LAN installations. Costs for applications, outsourcing and network management are critical factors that need to be considered before the wireless LAN can either supplement the wired LAN or replace it as a wired LAN alternative. These savings are substantial from the viewpoint of manufacturer, retailers, hospitals, schools, and financial organizations. A wireless LAN enables them to provide better quality goods, at reduced costs, in a significantly less time.

On average, the total cost per user was found to be $4550 for a wireless LAN solution. This includes the costs identified below (Note that the WLAN Hardware/End User Devices category includes the computing platform used, which was generally a handheld or laptop computer.) Wireless LAN infrastructure and end user devices account for the highest percentage cost out of this total. The percentages for wireless LAN expenses, by category, were as follows:

- WLANA Hardware/End User Devices: 50%
- Monthly expenses: 1%%
- Management expenses: 16%
- Application development expenses: 16% Outsourcing: 16% Downtime: 1%

d. Economic Benefits

With large investments in wireless LAN technology at approximately $300,000 to $4.2 million dollars per year, we clearly realize and sympathize with the managers that have been struggling to quantify the benefits that derive from wireless LANs. Organizations implementing an average of 300 client cards reaped annual savings of up to $4.9 million, which translated into per user savings of $15,989. As the wireless LAN solution is implemented on a large scale, these savings will eventually trickle down to the consumer.

e. Payback

Across all industries, the wireless LAN paid for itself within 12 months time. This is with all economic benefits considered. The payback period of this investment is the period of time required for the cumulative cash flows due to increased productivity, organizational efficiency and extra revenue/profit gain to equal the initial investment.

	Retail	Manufacturing	Health-care	Office Automation	Education
Benefits per company(millions $)	**5.6**	**2.2**	**.94**	**2.5**	**.5**
Costs per company(millions $)	**4.2**	**1.3**	**.90**	**1.3**	**.3**
Payback(# of months)	**9.7**	**7.2**	**11.4**	**6.3**	**7.1**

Figure 4.12. Cost Benefit Analysis. (Payback) (From Ref. 43).

With fast-rising healthcare costs, reimbursement and ROI are key to the requirements of IT investments in the medical industry. Healthcare spending in the U.S. has grown from $280 billion in 1981 to more than $1.5 trillion in 1997 and currently accounts for about 14% of the total gross domestic product. Due to healthcare costs increasing at a rate of about 5% per year, cost containment is an important issue. Hospitals are centralizing laboratories, reducing costs, and increasing their use of automated technology. The wireless LAN has shown to meet the technology and organizational needs of healthcare companies today by decreasing the length of hospital stay, speeding diagnostic and case analysis time turnaround, reducing hospital labor, procedural costs, documentation, and scheduling time. [43]

E. NETWORK DIAGRAM

1. Basic Architecture

Figure 4.14 is an example of how a standard WLAN architecture would look like. This is an example that an MTF can follow. A wireless network session will start with the wireless client establishing a connection with an access point within range. The negotiated session will be 128-bit WEP or WPA enabled. Further, if implemented, the access point will verify the client's MAC address to ensure it is authorized to access the network. At the same time, the RF monitor will detect the presence of the client and the access point and log appropriate audit information (i.e., MAC addresses, date/time detected). If the RF monitor detects any unauthorized MAC addresses, the event will be logged and a system administrator alerted as soon as possible (e.g., pager, e-mail). This alert mechanism could be accomplished by connecting the RF monitor with the local Network Operations Center (NOC). The switch/hub is not required for any security functions in this architecture; it is simply a pass-through device. The client will then authenticate itself with the access control device. The credentials in this transaction should be either certificate- or two-factor-based. The access control device will consult the authentication server for verification of the user's credentials and to provide authorization details. Regardless of whether the provided credentials are valid,

[43] Wireless LAN Association (WLANA). Wireless LAN Cost of Ownership Report. [http://www.wlana.org/learn/roi.htm.] Last accessed July 2004.

appropriate audit information (credentials, MAC address, date/timestamp) shall be logged by the authentication server. After authentication is complete, an encrypted tunnel will be generated between the access control device and the wireless client. The tunnel will be terminated at those devices and not extended to other devices. At this point, the wireless client has a secure connection to the internal network and should have access to any resources for which it has been authorized. For all LAN activity, a network intrusion detection system will monitor the network for suspicious traffic (i.e., possible attack scenarios including port scans, denial of service /syn floods). In addition, it will verify system integrity (e.g., system file changes) and log any auditable events.[44]

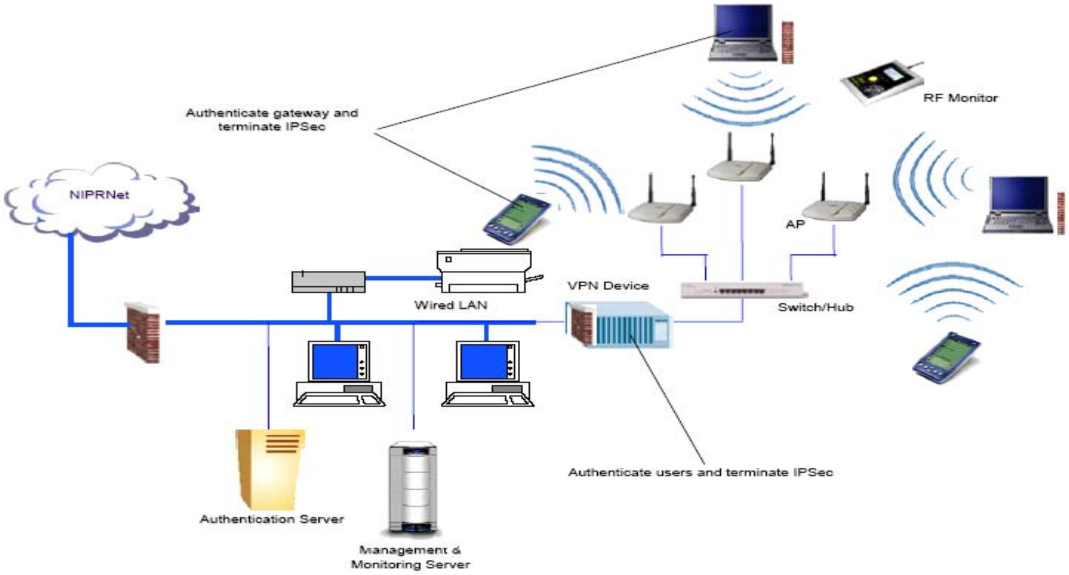

Authenticate gateway and terminate IPSec
RF Monitor
NIPRNet
AP
VPN Device
Wired LAN
Switch/Hub
Authenticate users and terminate IPSec
Authentication Server
Management & Monitoring Server

Figure 4.13 Basic Architecture (From Ref. 55).

F. SUMMARY

By looking at the data provided it can be seen that Naval Medicine can profit from incorporating WLANs into their current wired networks to provide greater redundancy along with cost savings. The studies show that it is possible to implement a

[44] DoD, DISA, Wireless Security Support Program. Wireless LAN Security Framework. Pg. 4-8 &– 4-9. January 2004.

WLAN without too much difficulty and receive an ROI within a year. Those who would benefit from this technology stand to gain an advantage in overall performance and cost throughout.

V. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

It is clear that WLAN technologies will be a part of every Naval MTF's daily operations. Many major hospitals throughout the United States have deployed 802.11 x technologies throughout their medical facilities. It is obvious that 802.11x will play a major role in the Naval MTF information system network architecture.

The needs and requirements for the deployment of 802.11x WLANs throughout all Naval MTFs focuses on the personnel that will be affected by the utilization of the network. These individuals are the main personnel who will conduct the day-to-day operations of the MTF that range from patient care, administration, to executive functions. The risks involved include the security of patient data, along with many other functions that exist beyond the scope of patient care.

The architectural design of the network is basic from the start. It will follow the basic wireless network setup and piggy back off of the original wired LAN. The needs and requirements for each MTF will determine any changes to the original design.

The benefits of developing and deploying a WLAN into the Naval MTF information network architecture is based on both physical and financial principles. The physical side offers less hardware infrastructure; therefore it is much more mobile throughout the MTF. The financial side offers a considerable savings and return on investment by cutting installation costs throughout.

The most important issue towards the deployment of WLANs in MTFs is policy. It can be its biggest proponent as well as its worst critic. Policy determines whether or not these networks will be arriving anytime soon. It plays a major factor in every aspect of government, and this is seen by the prohibition towards the use of WLANs in the past few years. Even though there are directives that specify the usage of the equipment it is still left up to the Designated Approving Authority of that region to decide who or what can be deployed at each respective command. This can be read in the messages in Appendix C and D, which are provided by COMNAVNETWARCOM NORFOLK VA. Naval MTFs now have the opportunity to deploy these networks throughout their clinics.

The DoD Directive 8100.2, April 14, 2004, signed by Deputy Secretary of Defense Paul Wolfowitz, allows for the use of Commercial Off-The-Shelf products to be used in DoD. Next, MTFs must follow the guidelines laid out in the Health Insurance and Portability Act of 1996 (HIPAA) to protect patient data that is maintained and distributed electronically. As long as the equipment complies with the previously mentioned directive and act, and meets the security requirements, they may be purchased and used.

From the data collected by the various papers, books, and articles, the use of 802.11x wireless LANs throughout Naval MTFs is possible. It is a cost effective method of providing the needed technology so health care providers, administrators, and executives can use it to optimize their MTFs performance. With the development of faster, smarter, more manageable equipment, WLANs are sure to grow within the MTFs. This, in turn, gives health care providers the necessary means to provide faster and more accurate patient care.

B. RECOMMENDATIONS

The following areas are for further research in regards to the development and deployment of WLANs in MTFs:

- 802.16 and its application towards MTFs and mobile medical platforms.
- Explore further issues of security and compliance with HIPAA.
- Explore the latest versions of tablet PCs and how they, along with software can provide a more efficient work place for health care providers.
- Creation of a comprehensive BUMED policy that provides guidelines for the development, deployment, and maintenance of WLANs.

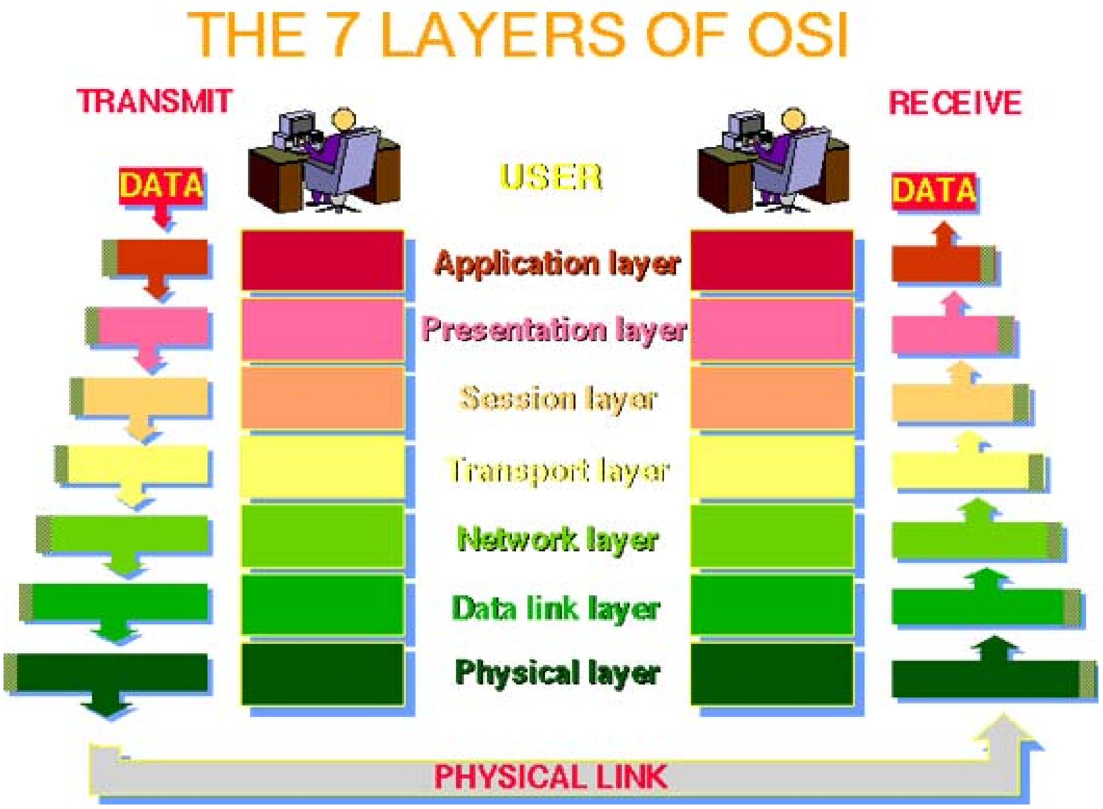
APPENDIX A

The 7 Layers of the OSI Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Application (Layer 7)	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
Presentation (Layer 6)	This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax layer*.
Session (Layer 5)	This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Transport (Layer 4)	This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
Network (Layer 3)	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
Data Link (Layer 2)	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The

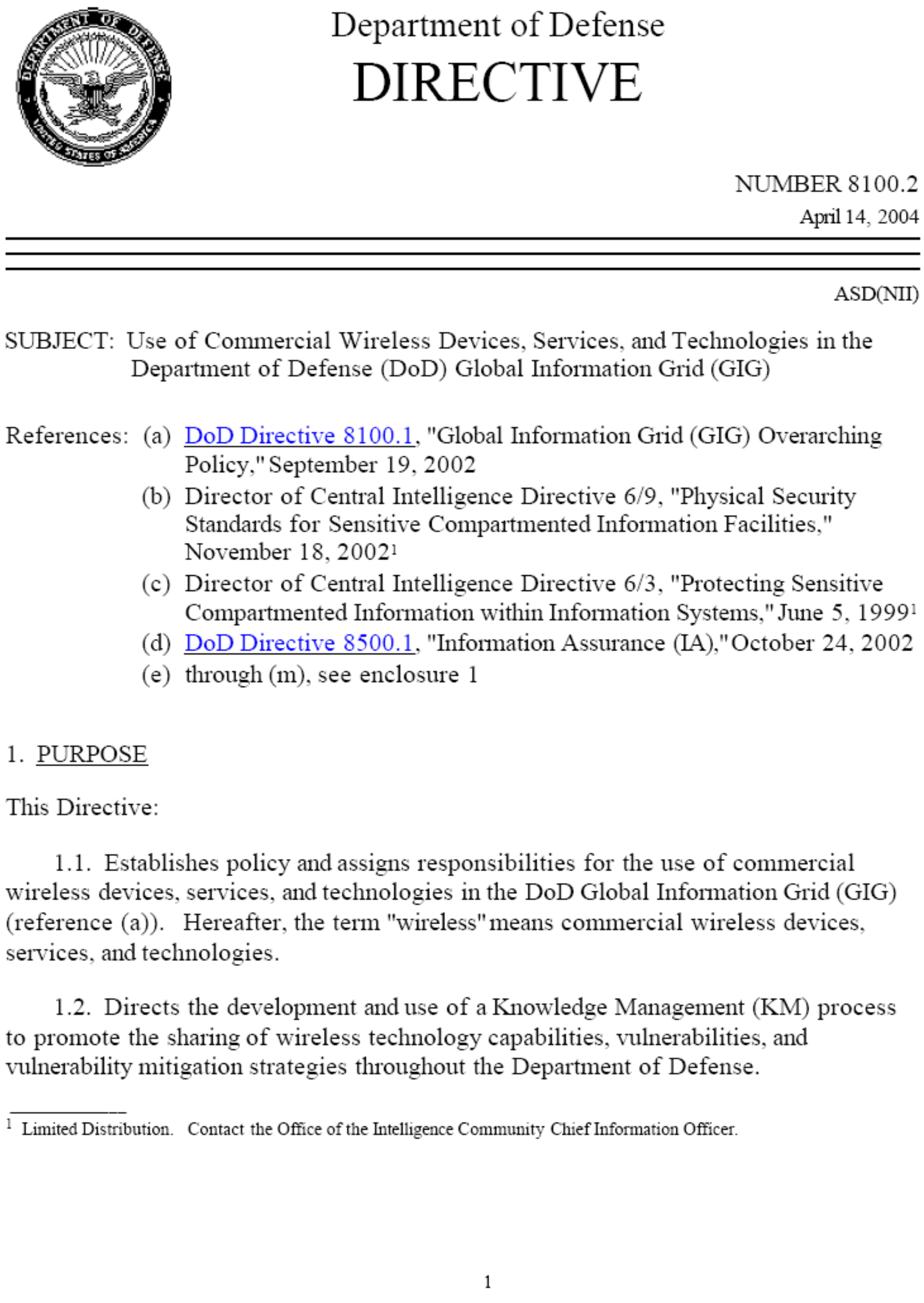
	Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
Physical (Layer 1)	This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.



This graphic is taken from The Abdus Salam International Centre for Theoretical Physics. [45]

[45] Webopedia. The 7 Layers of the OSI Model. [http://www.webopedia.com/quick_ref/OSI_Layers.asp]. July 2004.

APPENDIX B



Department of Defense

DIRECTIVE

NUMBER 8100.2
April 14, 2004

ASD(NII)

SUBJECT: Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

References:
(a) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(b) Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," November 18, 2002[1]
(c) Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 5, 1999[1]
(d) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(e) through (m), see enclosure 1

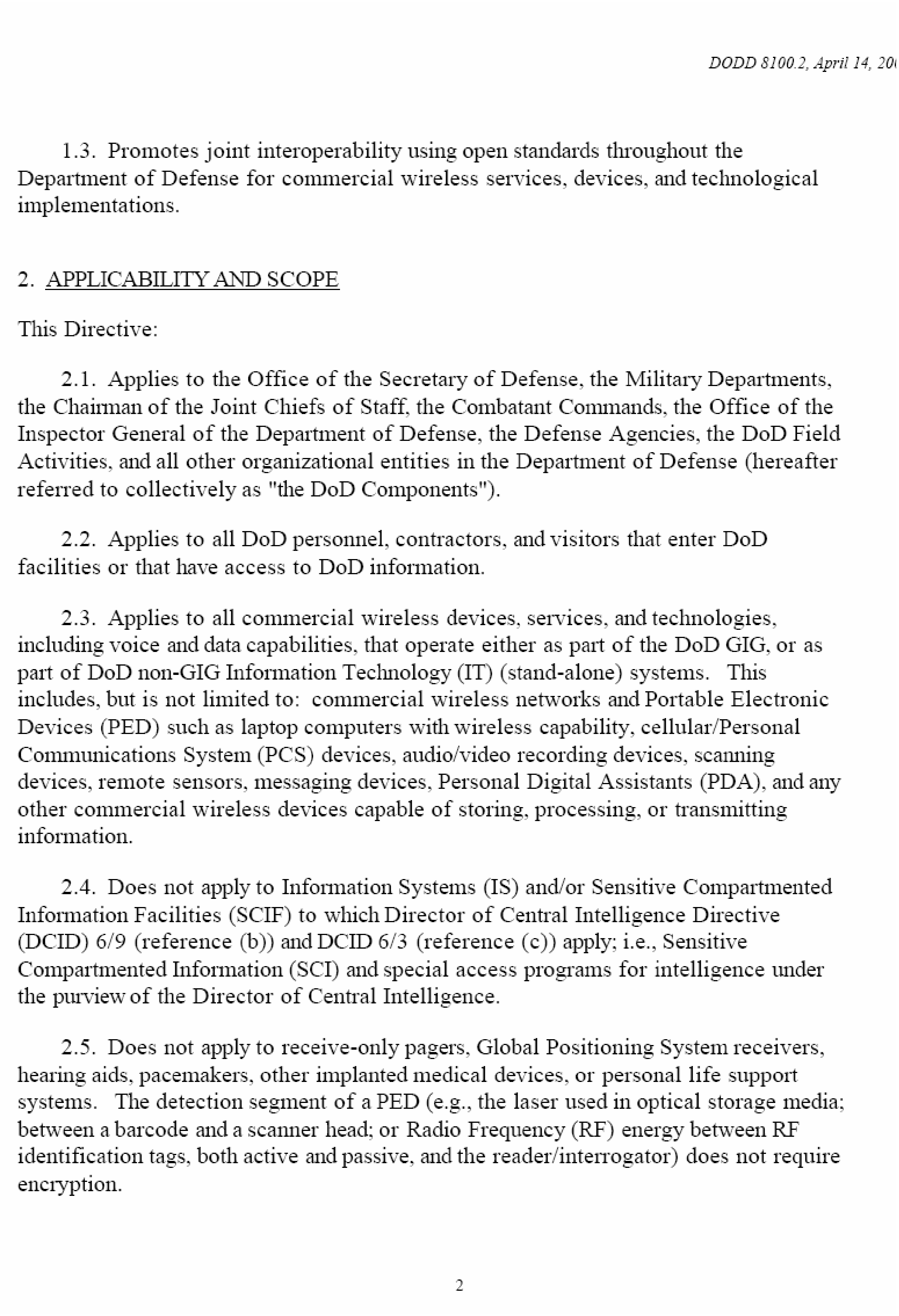
1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG) (reference (a)). Hereafter, the term "wireless" means commercial wireless devices, services, and technologies.

1.2. Directs the development and use of a Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department of Defense.

[1] Limited Distribution. Contact the Office of the Intelligence Community Chief Information Officer.



1.3. Promotes joint interoperability using open standards throughout the Department of Defense for commercial wireless services, devices, and technological implementations.

2. APPLICABILITY AND SCOPE

This Directive:

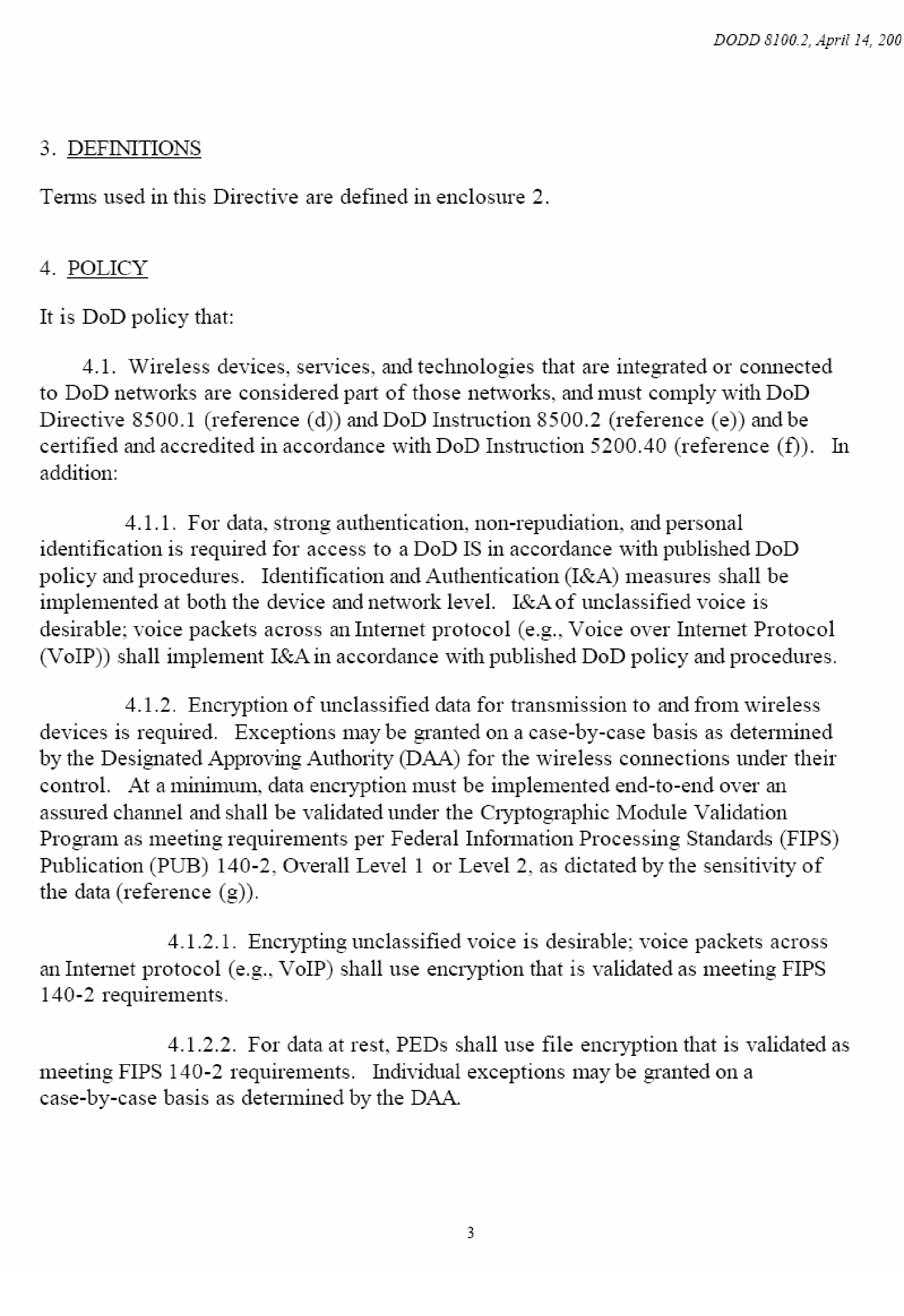
2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. Applies to all DoD personnel, contractors, and visitors that enter DoD facilities or that have access to DoD information.

2.3. Applies to all commercial wireless devices, services, and technologies, including voice and data capabilities, that operate either as part of the DoD GIG, or as part of DoD non-GIG Information Technology (IT) (stand-alone) systems. This includes, but is not limited to: commercial wireless networks and Portable Electronic Devices (PED) such as laptop computers with wireless capability, cellular/Personal Communications System (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDA), and any other commercial wireless devices capable of storing, processing, or transmitting information.

2.4. Does not apply to Information Systems (IS) and/or Sensitive Compartmented Information Facilities (SCIF) to which Director of Central Intelligence Directive (DCID) 6/9 (reference (b)) and DCID 6/3 (reference (c)) apply; i.e., Sensitive Compartmented Information (SCI) and special access programs for intelligence under the purview of the Director of Central Intelligence.

2.5. Does not apply to receive-only pagers, Global Positioning System receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems. The detection segment of a PED (e.g., the laser used in optical storage media; between a barcode and a scanner head; or Radio Frequency (RF) energy between RF identification tags, both active and passive, and the reader/interrogator) does not require encryption.



3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

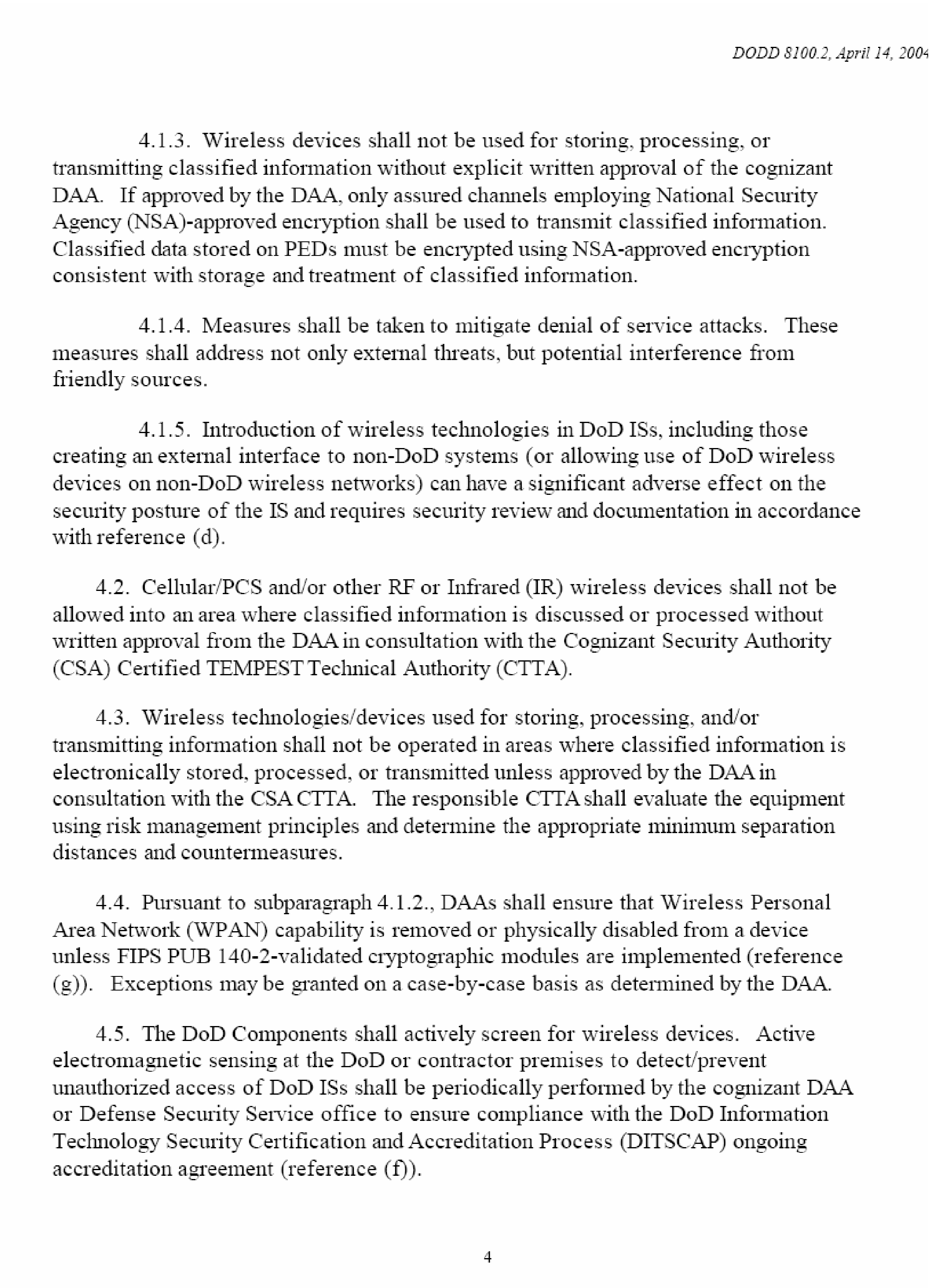
4.1. Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and must comply with DoD Directive 8500.1 (reference (d)) and DoD Instruction 8500.2 (reference (e)) and be certified and accredited in accordance with DoD Instruction 5200.40 (reference (f)). In addition:

4.1.1. For data, strong authentication, non-repudiation, and personal identification is required for access to a DoD IS in accordance with published DoD policy and procedures. Identification and Authentication (I&A) measures shall be implemented at both the device and network level. I&A of unclassified voice is desirable; voice packets across an Internet protocol (e.g., Voice over Internet Protocol (VoIP)) shall implement I&A in accordance with published DoD policy and procedures.

4.1.2. Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the Designated Approving Authority (DAA) for the wireless connections under their control. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (reference (g)).

4.1.2.1. Encrypting unclassified voice is desirable; voice packets across an Internet protocol (e.g., VoIP) shall use encryption that is validated as meeting FIPS 140-2 requirements.

4.1.2.2. For data at rest, PEDs shall use file encryption that is validated as meeting FIPS 140-2 requirements. Individual exceptions may be granted on a case-by-case basis as determined by the DAA.



4.1.3. Wireless devices shall not be used for storing, processing, or transmitting classified information without explicit written approval of the cognizant DAA. If approved by the DAA, only assured channels employing National Security Agency (NSA)-approved encryption shall be used to transmit classified information. Classified data stored on PEDs must be encrypted using NSA-approved encryption consistent with storage and treatment of classified information.

4.1.4. Measures shall be taken to mitigate denial of service attacks. These measures shall address not only external threats, but potential interference from friendly sources.

4.1.5. Introduction of wireless technologies in DoD ISs, including those creating an external interface to non-DoD systems (or allowing use of DoD wireless devices on non-DoD wireless networks) can have a significant adverse effect on the security posture of the IS and requires security review and documentation in accordance with reference (d).

4.2. Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA).

4.3. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

4.4. Pursuant to subparagraph 4.1.2., DAAs shall ensure that Wireless Personal Area Network (WPAN) capability is removed or physically disabled from a device unless FIPS PUB 140-2-validated cryptographic modules are implemented (reference (g)). Exceptions may be granted on a case-by-case basis as determined by the DAA.

4.5. The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at the DoD or contractor premises to detect/prevent unauthorized access of DoD ISs shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) ongoing accreditation agreement (reference (f)).

4.6. Mobile code shall not be downloaded from non-DoD sources. Downloading of mobile code shall only be allowed from trusted DoD sources over assured channels.

4.7. PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.

4.8. Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data, in accordance with reference (e). The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency.

4.9. The DoD Components shall seek and follow spectrum supportability guidance from the Military Communications-Electronics Board (MCEB) prior to assuming any contractual obligations for the full-scale development, production, procurement, or deployment of spectrum dependent (i.e., wireless) devices or systems, in accordance with DoD Directive 4650.1 (reference (h)).

4.10. A DoD wireless KM process shall be established. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.

4.10.1. The KM process shall be utilized by DAAs to help determine acceptable uses of wireless devices and employ appropriate mitigating actions.

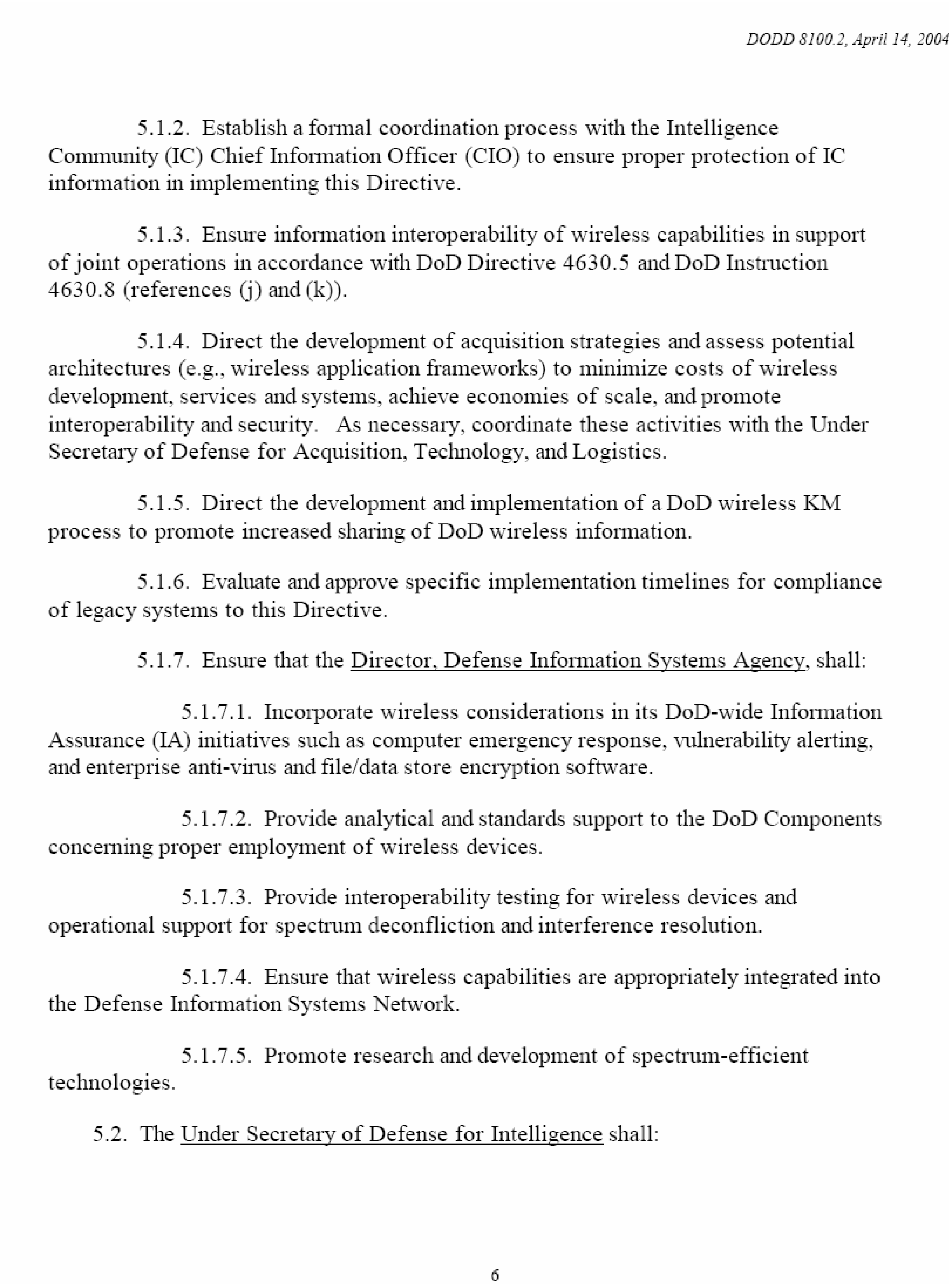
4.10.2. DAAs shall submit alternative mitigating techniques for inclusion in the KM database. The DoD Components shall use the KM process to coordinate, prioritize, and avoid duplication of vulnerability assessments of wireless devices.

4.10.3. Information on vulnerability assessments shall be considered for classification in accordance with DoD 5200.1-R (reference (i)) and handled appropriate to that classification.

5. <u>RESPONSIBILITIES</u>

5.1. The <u>Assistant Secretary of Defense for Networks and Information Integration</u>, as the <u>DoD Chief Information Officer</u>, shall:

5.1.1. Monitor and provide oversight and policy development of all DoD wireless activities.



5.1.2. Establish a formal coordination process with the Intelligence Community (IC) Chief Information Officer (CIO) to ensure proper protection of IC information in implementing this Directive.

5.1.3. Ensure information interoperability of wireless capabilities in support of joint operations in accordance with DoD Directive 4630.5 and DoD Instruction 4630.8 (references (j) and (k)).

5.1.4. Direct the development of acquisition strategies and assess potential architectures (e.g., wireless application frameworks) to minimize costs of wireless development, services and systems, achieve economies of scale, and promote interoperability and security. As necessary, coordinate these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics.

5.1.5. Direct the development and implementation of a DoD wireless KM process to promote increased sharing of DoD wireless information.

5.1.6. Evaluate and approve specific implementation timelines for compliance of legacy systems to this Directive.

5.1.7. Ensure that the Director, Defense Information Systems Agency, shall:

5.1.7.1. Incorporate wireless considerations in its DoD-wide Information Assurance (IA) initiatives such as computer emergency response, vulnerability alerting, and enterprise anti-virus and file/data store encryption software.

5.1.7.2. Provide analytical and standards support to the DoD Components concerning proper employment of wireless devices.

5.1.7.3. Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.

5.1.7.4. Ensure that wireless capabilities are appropriately integrated into the Defense Information Systems Network.

5.1.7.5. Promote research and development of spectrum-efficient technologies.

5.2. The Under Secretary of Defense for Intelligence shall:

5.2.1. Ensure that the Director, Defense Intelligence Agency, provides intelligence support and guidance on the use of wireless technologies for Defense Intelligence Agency-accredited SCIFs.

5.2.2. Ensure that the Director, Defense Security Service, includes monitoring and assessment of wireless IS security practices while conducting regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (l)).

5.2.3. Ensure that the Director, National Security Agency shall:

5.2.3.1. Implement a capability to assess the risks and vulnerabilities associated with wireless technologies that are responsive to DoD requirements.

5.2.3.2. Develop and disseminate threat information regarding the capabilities and intentions of adversaries to exploit wireless technologies used by the DoD Components.

5.2.3.3. Serve as the DoD focal point for IA wireless technologies research and development in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. As necessary, coordinate these activities with the Director, Defense Research and Engineering.

5.3. The OSD Principal Staff Assistants shall:

5.3.1. Ensure end-to-end protection and joint interoperability in their functional areas by guiding investments and other actions relating to wireless technologies.

5.3.2. Ensure wireless requirements for ISs and functional applications developed under their cognizance are fully coordinated at the DoD cross-Component level.

5.4. The Chairman of the Joint Chiefs of Staff shall:

5.4.1. Develop, coordinate, and promulgate wireless policies and procedures applicable to Joint operations.

5.4.2. Review, confirm, and certify the security and sufficiency of wireless-related interoperability requirements for ISs using wireless capabilities supporting Joint operations.

5.4.3. Ensure the appropriate review and confirmation of the sufficiency of wireless-related interoperability key performance parameters and information exchange requirements for all capstone requirements documents and operational requirements documents.

5.5. The Commander, U.S. Strategic Command, shall develop defensive actions necessary to detect, deter, or defeat unauthorized wireless activity up to and including computer network attacks against DoD computer networks and to minimize impact from such activities.

5.6. The Heads of the DoD Components shall:

5.6.1. Submit to the DoD CIO, within 180 days of this Directive, specific implementation timelines for compliance of legacy systems to this Directive.

5.6.2. Ensure that all new commercial wireless procurements comply with this Directive immediately. Ensure all entities within their organization and/or under their control that are involved in acquiring (e.g., either developing or procuring) spectrum-dependent (i.e., wireless) systems:

5.6.2.1. Seek and conform to guidance from the MCEB concerning the licensing and use of wireless systems.

5.6.2.2. Comply with the evaluation and validation requirements of enclosure 3 of reference (e).

5.6.3. Ensure use of the wireless KM process when evaluating potential wireless solutions.

5.6.4. Ensure that activities evaluating wireless technology provide feedback to the wireless KM process concerning strengths, weaknesses, vulnerabilities, mitigation techniques, and related security procedures.

5.6.5. Ensure that DAAs, in accordance with reference (f):

5.6.5.1. Control wireless access to ISs under their cognizance to ensure that the wireless systems (including external interfaces to commercial wireless services) do not introduce wireless vulnerabilities that undermine the assurance of the other interconnected systems.

5.6.5.2. Include intrusion detection methodologies for the wireless systems.

5.6.5.3. Incorporate wireless topics into annual IA training.

5.6.5.4. Review risk assessment results to make an informed and affirmative decision about the risk before granting an exception to this policy.

6. EFFECTIVE DATE

This Directive is effective immediately.

Paul Wolfowitz

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(f) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (supplemented by DoD 8510.1-M, "Application Manual," July 2000)

(g) Federal Information Processing Standard (FIPS) 140-2, May 25, 2001[2]

(h) DoD Directive 4650.1, "Management and Use of the Radio Frequency Spectrum," June 24, 1987

(i) DoD 5200.1-R, "Information Security Program," January 1997

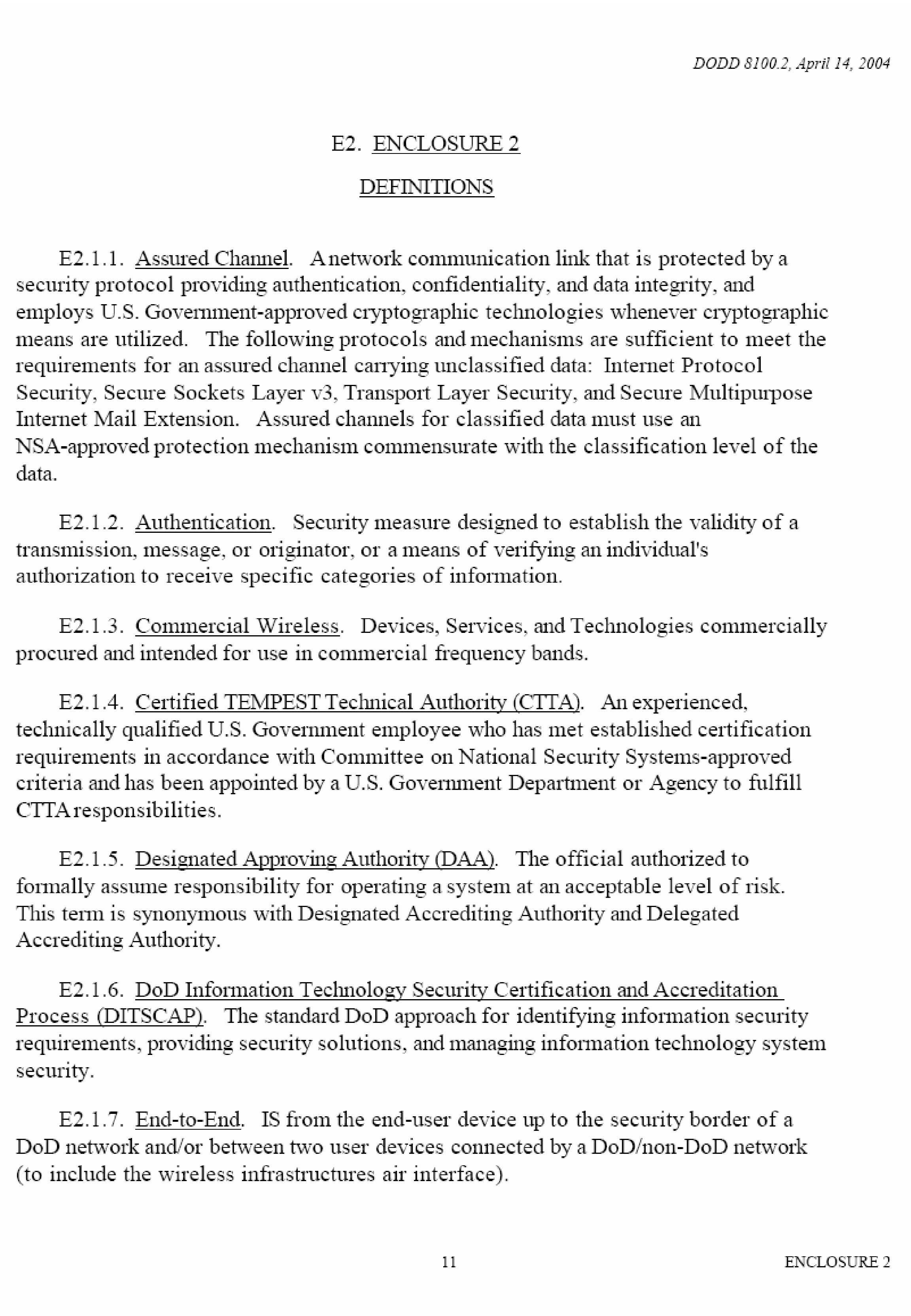
(j) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology and National Security Systems," January 11, 2002

(k) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology and National Security Systems," May 2, 2002

(l) DoD 5220.22-M, "National Industry Security Program Operating Manual," January 1995

(m) Section 11103(a) of title 40, United States Code

[2] Available via internet at http://www.itl.nist.gov/fipspubs/



E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Assured Channel. A network communication link that is protected by a security protocol providing authentication, confidentiality, and data integrity, and employs U.S. Government-approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements for an assured channel carrying unclassified data: Internet Protocol Security, Secure Sockets Layer v3, Transport Layer Security, and Secure Multipurpose Internet Mail Extension. Assured channels for classified data must use an NSA-approved protection mechanism commensurate with the classification level of the data.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

E2.1.3. Commercial Wireless. Devices, Services, and Technologies commercially procured and intended for use in commercial frequency bands.

E2.1.4. Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with Committee on National Security Systems-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

E2.1.5. Designated Approving Authority (DAA). The official authorized to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

E2.1.6. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security.

E2.1.7. End-to-End. IS from the end-user device up to the security border of a DoD network and/or between two user devices connected by a DoD/non-DoD network (to include the wireless infrastructures air interface).

E2.1.8. External Interfaces. Interfaces, including commercial systems (such as a cellular/PCS or pager network not under control of the DAA), capable of carrying traffic between systems under control of the DAA (e.g., the DoD IS and a DoD wireless device).

E2.1.9. Federal Information Processing Standards (FIPS). The standards issued by the National Institute of Standards and Technology for Federal computer systems (http:www.itl.nist.gov/fipspubs/).

E2.1.10. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in 40 U.S.C. 11103(a) (formerly section 5142 of the Clinger-Cohen Act of 1996) (reference (m)).

E2.1.10.1. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.10.1.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.10.1.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.10.1.3. Processes data or information for use by other equipment, software, and services.

E2.1.10.2. Non-GIG IT -- Stand-alone, self-contained, or embedded IT that is not or shall not be connected to the enterprise network.

E2.1.11. Heads of the DoD Components. For purposes of this policy guidance, the Heads of the DoD Components include: the Office of the Secretary of Defense Principal Staff Assistants, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, the Directors of the Defense Agencies and DoD Field Activities, and the Inspector General of the Department of Defense, and all other organizational entities in the Department of Defense.

E2.1.12. Identification & Authentication (I&A). Process of accepting a claimed identity and establishing the validity of that claimed identity.

E2.1.13. Information Assurance (IA). Measures used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.14. Information System (IS). The entire infrastructure, organization, personnel, and components used to collect, process, store, transmit, display, disseminate, and dispose of information.

E2.1.15. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. This includes equipment used by a DoD Component directly or used by a contractor under a contract with the DoD Component that:

E2.1.15.1. Requires the use of such equipment; or

E2.1.15.2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract (reference (a)).

E2.1.16. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

E2.1.17. Personal Digital Assistant (PDA). A generic term for a class of small, easily carried electronic devices used to store and retrieve information.

E2.1.18. Portable Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

E2.1.19. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.20. Spectrum Supportability. The assessment as to whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or a spectrum-dependent system during its expected life cycle is, or will be, available (that is, from system development, through development and operational testing, to actual operation in the electromagnetic environment). The assessment of "spectrum supportability" is based upon, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of electromagnetic compatibility (EMC).

E2.1.21. Synchronize. The process of communicating with a host or another PED to upload, download, merge, or swap information (Hot-Synch).

E2.1.22. Wireless. Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission.

E2.1.23. Wireless Personal Area Network (WPAN). A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either RF (e.g., Bluetooth) or IR technology.

APPENDIX C

-----Original Message-----

UNCLAS

ALCOM # 046-04

MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA/-/JUL//

SUBJ/ADDITIONAL GUIDANCE FOR WIRELESS LOCAL AREA NETWORK (WLAN) MORATORIUM//

REF/A/MSG/COMNAVNETWARCOM NORFOLK VA/021619ZJUL2004//

REF/B/MSG/COMPACFLT/192206ZAUG2003//

REF/C/MSG/COMFLTFORCOM/021742ZAPR2004//

REF/D/INST/DOD/14APR2004/8100.2//

REF/E/INST/CLF-CPF/27APR2000/4720.3A//

NARR/REF A IS THE ASHORE WIRELESS CESSATION MORATORIUM MSG, REFS B AND C ARE THE COMPACFLT/COMFLTFORCOM MSG CESSSATION OF WIRELESS LOCAL AREA NETWORK INSTALLATIONS IN COMPACFLT AND COMLANTFLT SHIPS, REF D IS USE OF COMMERCIAL WIRELESS DEVICES, SERVICES, AND TECHNOLOGIES IN DOD GRID, REF E IS MANAGEMENT OF AFLOAT COMBAT

SYSTEMS AND C4I INSTALLATIONS AND IMPROVEMENTS//

POC/GRETCHEN MERRYMAN/CDR/NNWC DEPUTY DAA/LOC:NAB LTLC/TEL:757-417-7912/EMAIL:GRETCHEN.MERRYMAN(AT)NAVY.MIL//

POC/DONALD KERRIGAN/CAPT/NNWC DAA/LOC:NAB LTLC/TEL:757-417-6740

/EMAIL:DONALD.KERRIGAN(AT)NAVY.MIL//

RMKS/1. PER REFS A THROUGH C, NEW WIRELESS 802.11 SYSTEMS/EQUIPMENT CANNOT BE PROCURED OR IMPLEMENTED, ASHORE OR AFLOAT WITHOUT OBTAINING APPROVAL FROM COMNAVNETWARCOM. IAW REF D, COMNAVNETWARCOM, AS THE NAVY DAA, HAS THE RESPONSIBILITY FOR CONTROLLING WIRELESS ACCESS TO NAVY INFORMATION SYSTEMS TO ENSURE

THAT THESE SYSTEMS (INCLUDING EXTERNAL INTERFACES TO COMMERCIAL WIRELESS SERVICES) DO NOT INTRODUCE VULNERABILITIES THAT UNDERMINE THE ASSURANCE OF INTERCONNECTED SYSTEMS. THE SCOPE OF THIS MORATORIUM INCLUDES BUT IS NOT LIMITED TO COMMERCIAL WIRELESS TECHNOLOGIES AND THEIR DERIVATIVES, AS STANDARDIZED IN IEEE

STANDARDS 802.11, 802.15 AND 802.16 COMMERCIAL WIRELESS DEVICES, SERVICES, AND TECHNOLOGIES, VOICE AND DATA CAPABILITIES, THAT OPERATE EITHER AS PART OF THE NAVY IT ENTERPRISE NETWORK OR STAND-ALONE SYSTEMS. THIS INCLUDES BUT IS NOT LIMITED TO PARA 2.3 OF REF D:

A. WIRELESS TECHNOLOGIES THAT FALL WITHIN THE SCOPE OF THIS MORATORIUM ARE AS FOLLOWS: A) THOSE THAT CAN PERMIT ACCESS TO NAVY INFORMATION

SYSTEMS WITHOUT TRANSITING AN EXISTING WIRED NETWORK ACCESS INTERFACE FOR REMOTE CONNECTIVITY, B) THOSE THAT CAN PROVIDE ACCESS TO UNCLASSIFIED DATA STORED ON PORTABLE OR STATIONARY ELECTRONIC DEVICES, AND C) THOSE THAT DO NOT PROTECT THE PRIVACY AND INTEGRITY OF DATA IN TRANSIT (I.E. TRANSMITTING OFFICIAL EMAIL INFORMATION IN THE CLEAR WITHOUT APPROVED CRYPTOGRAPHY). PER PARA 4.1.2 OF REF D, EXCEPTIONS MAY BE GRANTED ON A CASE-BY-CASE BASIS AS DETERMINED BY THE NAVY DAA.

B. WHAT IS NOT IN THE SCOPE OF THIS MORATORIUM AS OUTLINED IN PARA 2.5 OF REF D: CELLULAR VOICE PHONES, COMMERCIAL PACKET RADIO TECHNOLOGY BETWEEN A NAVY LAN AND A PED THAT 1) DOES NOT STORE INFORMATION, 2) PROTECTS ALL TRANSMISSIONS, AND 3) ACCESSES THE NAVY LAN THROUGH AN EXISTING, APPROVED WIRED, REMOTE NETWORK ACCESS SERVICE.

2. CURRENTLY DEPLOYED WIRELESS NETWORKS AND WIRELESS EXTENSIONS TO WIRED NETWORKS MAY CONTINUE TO OPERATE UNDER EXISTING APPROVED IATO/ATO. HOWEVER, THEY MUST BE REGISTERED NLT 30 AUG 2004. REGISTRATION IS REQUIRED IAW PARA 3. IN ADDITION TO PARA 3, COMNAVNETWARCOM HAS RESPONSIBILITY TO IDENTIFY, APPROVE AND ENSURE ALL WIRELESS DEVICES ARE OPERATING IAW REF D. EXISTING SSAA'S, IATO' S AND ATO'S MUST BE SUBMITTED FOR REGISTRATION VIA EMAIL TO THE COMNAVNETWARCOM POC IN PARA 5.

3. APPROVAL/WAIVER/REGISTRATION SUBMISSION FOR NEW OR EXISTING WIRELESS SYSTEMS MUST BE VIA NAVAL MESSAGE WITH A SUBJECT LINE OF "WIRELESS APPROVAL/WAIVER/REGISTRATION" TO COMNAVNETWARCOM NORFOLK VA/NSD/ USING THE SAMPLE A-O FORMAT BELOW IAW REF E.

A. COMMAND NAME, UIC, LOCATION OF NETWORK (BASE, BUILDING, ROOM)

B. CURRENT OR PROPOSED ARCHITECTURE INCLUDING: TYPE OF HARDWARE, SOFTWARE, FIRMWARE, IDS OR OTHER SECURITY FEATURES, SPECIFIC ENCRYPTION ALGORITHM UTILIZED, AND CLASSIFICATION OF DATA TO BE PROCESSED (SUBMISSION OF EXISTING SSAA WILL SUFICE)

C. JUSTIFICATION OF WIRELESS CAPABILITY (PURPOSE OF INSTALLATION)

D. OPERATIONAL IMPACT IF NOT INSTALLED

E. PREREQUISITE REQUIREMENTS (I.E. SPECIAL ADMINISTRATOR TRAINING, TEMPEST, HERO, HERF, RFI)

F. TESTING ACCOMPLISHED FOR APPROVAL/CERTIFICATION BY APPROPRIATE TECHNICAL AGENT (NAVSEA, SPAWAR, PEOS, ETC)

G. SCHEDULE (TO INCLUDE LENGTH OF TIME FOR TEMPORARY INSTALLATIONS, PROOF OF CONCEPT/DEPLOYMENT DATE)

H. INTEGRATED LOGISTICS SUPPORT REQUIREMENTS

I. TRAINING REQUIREMENTS

J. IMPACT TO EXISTING SYSTEMS

K. RISK ASSESSMENT

L. CONTINGENCY (OPTIONS/FALL BACK)

M. DOCUMENTATION REQUIREMENTS

N. INTEROPERABILITY IMPACT

O. POINT OF CONTACT, EMAIL AND PHONE NUMBER

4. WAIVER REQUEST SUBMITTED TO THIS MORATORIUM WILL BE CONSIDERED ON A CASE-BY-CASE BASIS VIA MSG AND MUST BE APPROVED IN WRITING BY THE NAVY DAA.

5. POC FOR REGISTRATION AND DOCUMENTATION IS: LEIGH ARMISTEAD/CIV/COMNAVNETWARCOM/LOC:NORFOLK VA/TEL:757-417-7914 EXT 1/EMAIL:EDWIN.ARMISTEAD(AT)NAVY.MIL OR CARRIE WATSON/CONT/COMNAVNETWARCOM/LOC:NORFOLK VA/TEL:757-417-6776 EXT 5/EMAIL:CARRIE.WATSON@NAVY.MIL//

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

R 021619Z JUL 04

FM COMNAVNETWARCOM NORFOLK VA

TO ALCOM

ENT/OU=DOD/OU=NAVY/OU=ADDRESS LISTS(UC)/CN=AL ALCOM(UC)

INFO ZEN/COMNAVNETWARCOM NORFOLK VA

DON CIO WASHINGTON DC

UNCLAS

SUBJ: WIRELESS LOCAL AREA NETWORK (WLAN) ASHORE MORATORIUM

UNCLASSIFIED//

UNCLAS

ALCOM # 038/04

THIS IS A NUMBERED ALCOM.

PASS TO OFFICE CODES

INFO COMNAVNETWARCOM NORFOLK VA//CIO/NSD//

DON CIO WASHINGTON DC//CIO//

MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA/-/JUL//

SUBJ/WIRELESS LOCAL AREA NETWORK (WLAN) ASHORE MORATORIUM//

REF/A/GENADMIN/COMPACFLT/192206ZAUG2003//

REF/B/GENADMIN/COMFLTFORCOM/021742ZAPR2004//

NARR/REFS A AND B ARE COMPACFLT/COMFLTFORCOM MSG CESSATION

OF

WIRELESS LOCAL AREA NETWORK INSTALLATIONS IN COMPACFLT AND

COMLANTFLT SHIPS//

POC/GRETCHEN MERRYMAN/CDR/NNWC DEPUTY DAA/LOC:NAB LTLC

/TEL:757-417-7912/EMAIL:GRETCHEN.MERRYMAN(AT)NAVY.MIL//

POC/DONALD KERRIGAN/CAPT/NNWC DAA/LOC:NAB LTLC/TEL:757-417-6740

/EMAIL:DONALD.KERRIGAN(AT)NAVY.MIL//

RMKS/1. REFS A AND B PROVIDED AN INITIAL MORATORIUM ON

SHIPBOARD

WLANS. NAVNETWARCOM CONCURS WITH THE NEED TO SECURE THE

NAVY

ENTERPRISE AGAINST WLANS VULNERABILITIES. THIS MESSAGE

EXTENDS THE

WLAN MORATORIUM TO ALL ASHORE COMMANDS AND ENTERPRISES

INCLUDING

BLII, NMCI, AND LEGACY NETWORKS. THIS MORATORIUM WILL REMAIN

IN

EFFECT UNTIL SECNAV AND NAVNETWARCOM ISSUE POLICIES ON

SECURING

WLANS IN THE DON ENTERPRISE.

2. WIRELESS SIGNALS ARE RADIO TRANSMISSIONS THAT CAN BE

INTERCEPTED

OR INTENTIONALLY JAMMED AND/OR EXPLOITED. EXPOSURE OF DATA IS

NOT

THE ONLY WLAN CONCERN FOR THE NAVY. IF IMPROPERLY

IMPLEMENTED, A

WIRELESS NETWORK ALLOWS AN UNAUTHENTICATED OR

UNAUTHORIZED USER

ACCESS TO THE NETWORK.

3. THIS MORATORIUM APPLIES TO ALL 802.11 WIRELESS INSTALLATIONS

AND

EQUIPMENT THAT OPERATE IN THE ISM OR UNII FREQUENCY BANDS

WHICH

COVER 900 MHZ, 2.4 GHZ AND 5.8 GHZ.

4. EXCEPTIONS TO THIS MORATORIUM WILL BE CONSIDERED ON A CASE

BY

CASE BASIS AND MUST BE APPROVED IN WRITING BY NAVNETWARCOM

NAVY

DAA.//

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Directive, Department of Defense, 8100.2. *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*. Pg. 1. April 14, 2004.

2. Naval Network Warfare Command. Subj: Additional Guidance for Wireless Local Area Network (WLAN) Moratorium. MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA/-/JUL//. Last accessed July 2004.

3. AirMagnet. *Wi-Fi, Health Care, and HIPAA: WLAN Management in the Modern Hospital.* Pg.1. Last accessed July 2004.

4. Gainer, Randy, van Eckhardt, Michael, Will, Rebecca, Marks, Richard. *HIPAA and WiFi – Regulatory Tangles for Wireless Health Care Networks*. [http://articles.corporate.findlaw.com/articles/file/00010/008895]. Last accessed July 2004.

5. O'Dorisio, Daniel. *Securing Wireless Networks for HIPAA Compliance.* Version 1.4 Option 2 (Case Study). SANS Institute. Pg. 3. December 23, 2003.

6. Geier, Jim. *Applications of Wireless Networks*. [http://www.wireless-nets.com/papers/wireless_network_applications.htm]. Last accessed July 2004.

7. Wheat, J. and others. *Designing a Wireless Network.* Pg. 125-126. Syngress, 2002.

8. Geier, Jim. *Wireless LANs: Implementing High Performance IEEE 802.11 Networks.* Second Edition. Pg.77-78. SAMS Publishing. 2002

9. IBM. *The 802.11g standard – IEEE.* [http://www-106.ibm.com/developerworks/wireless/library/wi-ieee.html]. March 2003.

10. Wi-Fi Planet. *AES*. [http://wi-fiplanet.webopedia.com/TERM/A/AES.html]. October 2003.

11. Mitchell, Bradley. *"WPA - Wi-Fi Protected Access"*. [http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm]. Last accessed July 2004.

12. Geier, Jim. *Wireless LANs: Implementing High Performance IEEE 802.11 Networks.* Second Edition. Pg.13. SAMS Publishing. 2002.

13. Geier, Jim. *Wireless LANs: Implementing High Performance IEEE 802.11 Networks.* Second Edition. Pg.31. SAMS Publishing. 2002.

14. Mitchell, Bradley. *Switches*.[http://comnetworking.about.com/library/glossary/bldef-switch.htm]. Last accessed July 2004.

15. Network Interface Cards. [http://www.webopedia.com/TERM/n/network_interface_card_NIC.html]. Last accessed July 2004.

16. Gilfor, Jeff Dr. *Wireless devices and Electromagnetic Interference in Hospitals, Urban Myth?* [http://www.pdamd.com/features/interference.xml]. Pg. 1. July 2004.

17. MDA. *MOBILE COMMUNICATIONS: INTERFERENCE WITH MEDICAL DEVICES.* [http://www.medical-devices.gov.uk/mda/mdawebsitev2.nsf/0/483b6bb5b6fbc80780256c8b003c88f3/$FILE/sn9706.pdf] April1997.

18. Osbourne. *CWNA, Certified Wireless Network Administrator*. McGraw Hill. 2003.

19. Räty, J. and Kaukinen, S. *Defeating Security in Wireless LANs.* Pg. 3 Last accessed July 2004.

20. Emigh, J. *WPA: Is Wi-Fi's Security Bandage Going to Win Over Network Admins?* [http://www.wi-fiplanet.com/tutorials/article.php/1550561]. December 2002.

21. Arbaugh W. *Your 802.11 Wireless Network Has No Clothes.* [http://www.drizzle.com/~aboba/IEEE/wireless.pdf]. March 2001.

22. Fluhrer, Mantin, and Shamir. *Weakness in the Key Scheduling Algorithm of RC4* [http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf]. August 2001.

23. Stubblefield, A. *Using Fluhrer, Mantin, and Shamir Attack to Break WEP.* [http://www.cs.rice.edu/~astubble/wep]. August 2001.

24. Walker, J. *Unsafe at Any Key Size; An Analysis of the WEP Encapsulation,* [http://www.drizzle.com/~aboba/IEEE/0-362.zip]. October 2000.

25. Roth, Joseph L., *Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions.*

Master's Thesis. Naval Postgraduate School. Monterey, California. Pg. 44-46. September 2002.

26. Internet.com. Webopedia. *WPA*. [http://www.webopedia.com/TERM/W/WPA.html]. Last accessed July 2004.

27. Virtual Private Networks. [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm#xtocid2]. Last accessed July 2004.

28. Dictionary.com. *VPN*. [http://dictionaryreference.com/search?q=virtual+private+network&r=67]. Last accessed July 2004.

29. Cites. VPN networking diagram. [http://www.cites.uiuc.edu/vpn/vpnnetdiagram.html]. Last accessed July 2004.

30. Internet.com. Webopedia. *Secure Shell (SSH)*. [http://www.webopedia.com/TERM/S/SSH.html]. Last accessed July 2004.

31. Pragma Systems Inc. *Secure Shell (sshd) Server for Windows NT/2000/XP*. Pg. 1. August 2001.

32. Fewer, S. SSL. *A discussion of the secure socket layer*. [http://harmony.hazors.com] Last accessed July 2004.

33. Internet.com. Webopedia. *Intrusion Detection Systems.* [http://www.webopedia.com/TERM/I/intrusion_detection_system.html]. Last accessed July 2004.

34. ReefEdge. Site Manager Software. [http://www.reefedge.com/reefedge/apm.do]. Last accessed July 2004.

35. AirDefense. Features. [http://www.airdefense.net/products/features/security.html]. Pg. 2-3. Last accessed July 2004.

36. Geroski, R. TechRepublic.com. AirDefense. Diagram. [http://techrepublic.com.com/5100-6264-1059473.html]. Pg. 1. November 2002.

37. Roth, Joseph L., *Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions.* Master's Thesis. Naval Postgraduate School. Monterey, California. Pg. 69. September 2002.

38. Roth, Joseph L., *Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions.* Master's Thesis. Naval Postgraduate School. Monterey, California. Pg. 78. September 2002.

39. *2003 Wireless LAN Benefits Study.* NOP World-Technology and Cisco Systems. [http://www.cisco.com/application/pdf/en/us/guest/products/ps4570/c1031/cdccont_0900aecd800cf9lf.pdf]. November 2003.

40. NETEAM. *Making a Case for Wireless Technology in Patient Safety.* Pg. 7. March 2004.

41. NETEAM. Making a Case for Wireless Technology in Patient Safety. Pg. 7. March 2004.

42. Kleinberg, K. *Mobile Healthcare: Applications, Vendors and Adoption.* [http://www.himss.org/content/files/proceedings/2003/Sessions/session102_slides.pdf]. Last accessed July 2004.

43. Wireless LAN Association (WLANA). *Wireless LAN Cost of Ownership Report.* [http://www.wlana.org/learn/roi.htm. Last accessed July 2004.

44. DoD, DISA, Wireless Security Support Program. *Wireless LAN Security Framework*. Pg. 4-8, 4-9, & 4-11. January 2004.

45. Webopedia. The 7 Layers of the OSI Model. [http://www.webopedia.com/quick_ref/OSI_Layers.asp]. Last accessed July 2004.

46. 3Com. Image. [http://www.3com.com/corpinfo/en_US/pressbox/resources/lan_switch_sta.html]. Last accessed July 2004.

47. D-Link. Image. [http://www.dlink.com/products?pid=13]. Last accessed July 2004.

48. Linksys. Image. [http://www.linksys.com/Products/product.asp?prid=508&scid=35]. Last accessed July 2004.

49. Dell. Image. [http://search.dell.com/results.aspx?cat=all&s=gen&c=us&l=en&cs=&k=Trumobile&x=0&y=0]. Last accessed July 2004.

50. Diagram of SSL operation. [http://www.harmony.hazors.com]. Last accessed July 2004.

51. Cisco Systems. IDS Diagram. [www.cisco.com]. Last accessed July 2004.

52. AirDefense.com. Diagram. [http://www.airdefense.net/products/]. Last accessed July 2004.

53. Webopedia. The 7 Layers of the OSI Model. [http://Webopedia.com/quick_ref/OSI_Layers.asp]. Last accessed July 2004.

54. Cisco Systems. *2003 Wireless LAN Benefits Study.* November 2003.

55. DISA, Wireless LAN Security Framework. Pg. 4-11. January 2004.

56. Intel Pro Network Connections. [http://www.intel.com/network/connectivity/resources/doc_library/data_sheets/NP169003.pdf]. Last accessed July 2004.

57. Cisco Aironet 1200 Series Access Point. [http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/casap_ds.htm]. Last accessed July 2004.

58. HP ProCurve Wireless Enterprise AP. [http://www.costcentral.com/prod/HP/J8133A/876013/0/0/yahoo]. Last accessed July 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

AirDefense. Diagram. [http://www.airdefense.net/products/]. Last accessed July 2004.

AirDefense. Features. [http://www.airdefense.net/products/features/security.html]. Last accessed July 2004.

AirMagnet. *Wi-Fi, Health Care, and HIPAA: WLAN Management in the Modern Hospital.* Last accessed July 2004.

Arbaugh W. *Your 802.11 Wireless Network Has No Clothes.* [http://www.drizzle.com/~aboba/IEEE/wireless.pdf]. March 2001.

Bogen, Jon. *Now comes the security challenge.* SC Magazine. April 2003.

Building a Cisco Wireless LAN
by Ron Fuller, Tim Blankenship

Cap Gemini Ernst & Young Guide to Wireless Enterprise Application Architecture
by Adam Kornak, John Distefano

Carnegie Mellon University. *Welcome to Wireless Andrew.* [http://www.cmu.edu/computing/wireless]. August 2002.

Cisco Aironet 1200 Series Access Point. [http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/casap_ds.htm]. Last accessed July 2004.

Cisco Systems. IDS Diagram. [www.cisco.com]. Last accessed July 2004.

Cisco Systems. *2003 Wireless LAN Benefits Study.* November 2003.

Cites. VPN networking diagram. [http://www.cites.uiuc.edu/vpn/vpnnetdiagram.html]. Last accessed July 2004.

Dell. Image. [http://search.dell.com/results.aspx?cat=all&s=gen&c=us&l=en&cs=&k=Trumobile&x=0&y=0]. Last accessed July 2004.

Designing a Wireless Network
by Jeffrey Wheat, Randy Hiser, Jackie Tucker, Alicia Neely, Andy McCullough

Diagram of SSL operation. [http://www.harmony.hazors.com]. Last accessed July 2004.

Dictionary.com. *VPN.* [http://dictionaryreference.com/search?q=virtual+private+network&r=67]. Last accessed July 2004.

Directive, Department of Defense, 8100.2. *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*. April 14, 2004.

DISA, Wireless LAN Security Framework. January 2004.

D-Link. Image. [http://www.dlink.com/products?pid=13]. Last accessed July 2004.

DoD, DISA, Wireless Security Support Program. *Wireless LAN Security Framework*. January 2004.

Emigh, J. *WPA: Is Wi-Fi's Security Bandage Going to Win Over Network Admins?* [http://www.wi-fiplanet.com/tutorials/article.php/1550561]. December 2002.

Enterprise Integration: An Architecture for Enterprise Application and Systems Integration by Fred A. Cummins

Fewer, S. SSL. *A discussion of the secure socket layer*. [http://harmony.hazors.com] Last accessed July 2004.

Fluhrer, Mantin, and Shamir. *Weakness in the Key Scheduling Algorithm of RC4* [http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf]. August 2001.

Gainer, Randy, van Eckhardt, Michael, Will, Rebecca, Marks, Richard. *HIPAA and WiFi – Regulatory Tangles for Wireless Health Care Networks*. [http://articles.corporate.findlaw.com/articles/file/00010/008895]. Last accessed July 2004.

Gartner Research. *New 802.11i Standard Will Advance Wireless Networking.* [http://www4.gartner.com/resources/121600/121673/new_80211i_stan.pdf]. Last accessed July 2004.

Geier, Jim. *Applications of Wireless Networks*. [http://www.wireless-nets.com/papers/wireless_network_applications.htm]. Last accessed July 2004.

Geier, Jim. *Wireless LANs: Implementing High Performance IEEE 802.11 Networks.* Second Edition. SAMS Publishing. 2002

Geroski, R. TechRepublic.com. AirDefense. Diagram. [http://techrepublic.com.com/5100-6264-1059473.html. November 2002.

Gilfor, Jeff Dr. *Wireless devices and Electromagnetic Interference in Hospitals, Urban Myth?* [http://www.pdamd.com/features/interference.xml]. Last accessed July 2004.

Hakala, David. *Wireless: Big Business in Health Care.* [http://crn.channelsupersearch.com/news/var/38316.asp]. November 1, 2002.

HIPAA Security for Wireless Networks. NETMOTION Wireless. 2001.

HP ProCurve Wireless Enterprise AP. [http://www.costcentral.com/prod/HP/J8133A/876013/0/0/yahoo]. Last accessed July 2004.

IBM. The 802.11g standard – IEEE. [http://www-106.ibm.com/developerworks/wireless/library/wi-ieee.html]. March 2003.

Intel Pro Network Connections. [http://www.intel.com/network/connectivity/resources/doc_library/data_sheets/NP169003.pdf]. Last accessed July 2004.

Internet.com. Webopedia. *Intrusion Detection Systems.* [http://www.webopedia.com/TERM/I/intrusion_detection_system.html]. Last accessed July 2004.

Internet.com. Webopedia. *Secure Shell (SSH)*. [http://www.webopedia.com/TERM/S/SSH.html]. Last accessed July 2004.

Internet.com. Webopedia. *WPA*. [http://www.webopedia.com/TERM/W/WPA.html]. Last accessed July 2004.

IP-Based Next-Generation Wireless Networks : Systems, Architectures, and Protocols by Jyh-Cheng Chen, Tao Zhang

Keltner, Jason and Miller, Paul, *Integration of Personal Digital Assistant (PDA) Devices Into The Military Healthcare Clinic Environment. Master's Thesis*. Naval Postgraduate School. Monterey, California. September 2001.

Kleinberg, K. *Mobile Healthcare: Applications, Vendors and Adoption.* [http://www.himss.org/content/files/proceedings/2003/Sessions/session102_slides.pdf]. Last accessed July 2004.

Linksys. Image. [http://www.linksys.com/Products/product.asp?prid=508&scid=35]. Last accessed July 2004.

MDA. *MOBILE COMMUNICATIONS: INTERFERENCE WITH MEDICAL DEVICES.* [http://www.medical-devices.gov.uk/mda/mdawebsitev2.nsf/0/483b6bb5b6fbc80780256c8b003 c88f3/$FILE/sn9706.pdf] April1997.

Mitchell, Bradley. *Switches*.[http://comnetworking.about.com/library/glossary/bldef-switch.htm]. Last accessed July 2004.

Mitchell, Bradley. *"WPA - Wi-Fi Protected Access"*. [http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm]. Last accessed July 2004.

Naval Network Warfare Command. Subj: Additional Guidance for Wireless Local Area Network (WLAN) Moratorium. MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA/-/JUL//. Last accessed July 2004.

NETEAM. *Making a Case for Wireless Technology in Patient Safety.*. March 2004.

Network Interface Cards. [http://www.webopedia.com/TERM/n/network_interface_card_NIC.html]. Last accessed July 2004.

O'Dorisio, Daniel. *Securing Wireless Networks for HIPAA Compliance.* Version 1.4 Option 2 (Case Study). SANS Institute. December 23 2003.

Osbourne. *CWNA, Certified Wireless Network Administrator*. McGraw Hill. 2003.

Pragma Systems Inc. *Secure Shell (sshd) Server for Windows NT/2000/XP*. August 2001.

Räty, J. and Kaukinen, S. *Defeating Security in Wireless LANs.* Last accessed July 2004.

Roth, Joseph L., *Enterprise Implementations of Wireless Network Technologies At The Naval Postgraduate School and Other Military Educational Institutions.* Master's Thesis. Naval Postgraduate School. Monterey, California. September 2002.

ReefEdge. Site Manager Software. [http://www.reefedge.com/reefedge/apm.do]. Last accessed July 2004.

Securing Wireless LANs: A Practical Guide for Network Managers, LAN Administrators and the Home Office User.
by Gilbert Held

Stubblefield, A. *Using Fluhrer, Mantin, and Shamir Attack to Break WEP.* [http://www.cs.rice.edu/~astubble/wep]. August 2001.

The Wireless Mobile Internet: Architectures, Protocols and Services
by Abbas Jamalipour

Virtual Private Networks.
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm#xtocid2]. Last accessed July 2004.

Walker, J. *Unsafe at Any Key Size; An Analysis of the WEP Encapsulation,* [http://www.drizzle.com/~aboba/IEEE/0-362.zip]. October 2000.

Webopedia. The 7 Layers of the OSI Model.
[http://www.webopedia.com/quick_ref/OSI_Layers.asp]. Last accessed July 2004.

Wheat, J. and others. *Designing a Wireless Network.* Syngress, 2002.

Wi-Fi, Health Care, and HIPAA. WLAN Management in the Modern Hospital. AIRMAGNET. Last accessed May 2004.

Wi-Fi Planet. AES. [http://wi-fiplanet.webopedia.com/TERM/A/AES.html]. October 2003.

Wireless Internet Applications & Architecture (ELECTRONIC COPY: ISBN 0201733544)
by Mark Beaulieu

Wireless LAN Association (WLANA). *Wireless LAN Cost of Ownership Report.* [http://www.wlana.org/learn/roi.htm. Last accessed July 2004.

Wireless Lans: Implementing Interoperable Networks
by James T. Geier,

Wireless Networking Handbook
by James T. Geier,

2003 Wireless LAN Benefits Study. NOP World-Technology and Cisco Systems. [http://www.cisco.com/application/pdf/en/us/guest/products/ps4570/c1031/cdccont_0900aecd800cf9lf.pdf]. November 2003.

3Com. Image.
[http://www.3com.com/corpinfo/en_US/pressbox/resources/lan_switch_sta.html]. Last accessed July 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

4. Glenn Cook
   Naval Postgraduate School
   Monterey, California

5. LT Russell Deason
   Naval Postgraduate School
   Monterey, California